

.....  
(Original Signature of Member)

118TH CONGRESS  
1ST SESSION

**H. R.** \_\_\_\_\_

To provide for individual rights relating to privacy of personal information, to establish privacy and security requirements for covered entities relating to personal information, and to establish an agency to be known as the Digital Privacy Agency to enforce such rights and requirements, and for other purposes.

\_\_\_\_\_  
**IN THE HOUSE OF REPRESENTATIVES**

Ms. ESHOO introduced the following bill; which was referred to the Committee  
on \_\_\_\_\_  
\_\_\_\_\_

**A BILL**

To provide for individual rights relating to privacy of personal information, to establish privacy and security requirements for covered entities relating to personal information, and to establish an agency to be known as the Digital Privacy Agency to enforce such rights and requirements, and for other purposes.

1       *Be it enacted by the Senate and House of Representa-*  
2       *tives of the United States of America in Congress assembled,*

1 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

2 (a) SHORT TITLE.—This Act may be cited as the  
3 “Online Privacy Act of 2023”.

4 (b) TABLE OF CONTENTS.—The table of contents for  
5 this Act is as follows:

- Sec. 1. Short title; table of contents.
- Sec. 2. Definitions.
- Sec. 3. General provisions.
- Sec. 4. Limitation on disclosing nonredacted government records.
- Sec. 5. Privacy considerations for legislative branch agencies.
- Sec. 6. Criminal prohibition on doxxing.

**TITLE I—INDIVIDUAL RIGHTS**

- Sec. 101. Right of access.
- Sec. 102. Right of correction.
- Sec. 103. Right of deletion.
- Sec. 104. Right of portability.
- Sec. 105. Right to human review of automated decisions.
- Sec. 106. Right to individual autonomy.
- Sec. 107. Right to be informed.
- Sec. 108. Right to impermanence.
- Sec. 109. Exemptions, exceptions, fees, timelines, and rules of construction for rights under this title.

**TITLE II—REQUIREMENTS FOR COVERED ENTITIES, SERVICE PROVIDERS, AND THIRD PARTIES**

- Sec. 201. Minimization.
- Sec. 202. Minimization and records of access by employees and contractors.
- Sec. 203. Prohibitions on disclosing of personal information.
- Sec. 204. Disclosing to entities not subject to United States jurisdiction or not compliant with this Act.
- Sec. 205. Prohibition on reidentification.
- Sec. 206. Restrictions on collecting, processing, maintaining, and disclosing contents of communications.
- Sec. 207. Prohibition on discriminatory processing.
- Sec. 208. Requirements for notice and consent processes and privacy policies.
- Sec. 209. Prohibition on “dark patterns” in notice and consent processes and privacy policies.
- Sec. 210. Notice and consent required.
- Sec. 211. Privacy policy.
- Sec. 212. Information security requirements.
- Sec. 213. Notification of data breach or data-sharing abuse.

**TITLE III—DIGITAL PRIVACY AGENCY**

- Sec. 301. Establishment; director and deputy director.
- Sec. 302. Agency powers and authorities.
- Sec. 303. Reporting and audit requirements.
- Sec. 304. Relation to other agencies.

- Sec. 305. Personnel.
- Sec. 306. Office of Civil Rights.
- Sec. 307. Complaints of individuals.
- Sec. 308. Advisory boards.
- Sec. 309. Authorization of appropriations.

#### TITLE IV—ENFORCEMENT

- Sec. 401. Investigations and administrative discovery.
- Sec. 402. Hearings and adjudication proceedings.
- Sec. 403. Litigation authority.
- Sec. 404. Enforcement by States.
- Sec. 405. Private rights of action.
- Sec. 406. Relief available.
- Sec. 407. Referral for criminal proceedings.
- Sec. 408. Whistleblower enforcement.

#### TITLE V—RELATION TO OTHER LAW

- Sec. 501. Effective date.
- Sec. 502. Relation to other Federal law.
- Sec. 503. Relation to State law.
- Sec. 504. Severability.

#### TITLE VI—NIST AND NSF ACTIVITIES

- Sec. 601. National Institute of Standards and Technology privacy research and development.
- Sec. 602. National privacy awareness and education initiative.
- Sec. 603. National Science Foundation privacy research.

### 1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) AGENCY.—The term “Agency” means the  
4 Digital Privacy Agency established in section 301.

5 (2) AGENCY INVESTIGATOR.—The term “Agen-  
6 cy investigator” means any attorney or investigator  
7 employed by the Agency who is charged with the  
8 duty of enforcing or carrying into effect any provi-  
9 sion of this Act or a rule or order prescribed under  
10 this Act.

11 (3) BEHAVIORAL PERSONALIZATION.—

1 (A) IN GENERAL.—The term “behavioral  
2 personalization” means the processing of an in-  
3 dividual’s personal information, using an algo-  
4 rithm, model, or other means—

5 (i) built using—

6 (I) that individual’s personal in-  
7 formation collected over a period of  
8 time; or

9 (II) an aggregate of the informa-  
10 tion of one or more similarly situated  
11 individuals; and

12 (ii) designed to—

13 (I) alter, influence, guide, or pre-  
14 dict that individual’s behavior;

15 (II) tailor or personalize a prod-  
16 uct or service to that individual; or

17 (III) filter, sort, limit, promote,  
18 display or otherwise differentiate be-  
19 tween specific content or categories of  
20 content that would otherwise be acces-  
21 sible to that individual.

22 (B) EXCLUSIONS.—The term “behavioral  
23 personalization” does not include the use of his-  
24 torical personal information to merely prevent

1 the display of or provide additional information  
2 about previously accessed content.

3 (4) COLLECT.—The term “collect” includes,  
4 with respect to personal information or the contents  
5 of any communication, obtaining such information or  
6 contents in any manner, except when solely trans-  
7 mitting, routing, providing intermediate storage for,  
8 or providing connections for such personal informa-  
9 tion or communication through a system or network.

10 (5) COMMISSION.—The term “Commission”  
11 means the Federal Trade Commission.

12 (6) CONTENTS.—The term “contents”, when  
13 used with respect to communication, has the mean-  
14 ing given such term in section 2510 of title 18,  
15 United States Code.

16 (7) COVERED ENTITY.—

17 (A) IN GENERAL.—The term “covered en-  
18 tity” means a person who—

19 (i) intentionally collects, processes, or  
20 maintains personal information; and

21 (ii) sends or receives such personal in-  
22 formation over the internet or a similar  
23 communications network.

24 (B) EXCLUSION.—The term “covered enti-  
25 ty” does not include a natural person, except to

1           the extent such person is engaged in a commer-  
2           cial activity that is more than de minimis.

3           (8) CUSTODIAN.—The term “custodian” means  
4           the custodian or any deputy custodian designated by  
5           the Agency.

6           (9) DATA BREACH.—The term “data breach”  
7           means unauthorized access to or acquisition of per-  
8           sonal information or contents of communications  
9           maintained by such covered entity.

10          (10) DATA-SHARING ABUSE.—The term “data-  
11          sharing abuse” means processing, by a third party,  
12          of personal information or contents of communica-  
13          tions disclosed by a covered entity to the third party,  
14          for any purpose other than—

15                (A) a purpose specified by the covered en-  
16                tity to the third party at the time such personal  
17                information or contents of communications was  
18                disclosed; or

19                (B) a purpose to which the individual to  
20                whom the information relates has consented.

21          (11) DE-IDENTIFY.—

22                (A) IN GENERAL.—The term “de-identify”  
23                means, with respect to information, performing  
24                actions so that such information cannot reason-  
25                ably identify, relate to, describe, reference, be

1           capable of being associated with, or be linked,  
2           directly or indirectly, to a particular individual  
3           or device, but only to the extent that the cov-  
4           ered entity that uses such information—

5                   (i) has performed such actions using  
6                   best practices for the types of data such  
7                   information contains;

8                   (ii) has implemented technical safe-  
9                   guards that prohibit re-identification of the  
10                  individual with whom such information was  
11                  linked;

12                  (iii) has implemented business proc-  
13                  esses that specifically prohibit re-identifica-  
14                  tion of the information;

15                  (iv) has implemented business proc-  
16                  esses to prevent inadvertent release of such  
17                  information; and

18                  (v) makes no attempt to re-identify  
19                  such information.

20           (B) DETERMINATION BY THE DIRECTOR.—

21           The Director may determine that a method-  
22           ology of de-identifying personal information is  
23           insufficient for the purposes of this paragraph.

24           (12) DIRECTOR.—The term “Director” means  
25           the Director of the Agency.

1           (13) DISCLOSE.—The term “disclose” means,  
2           with respect to personal information or contents of  
3           communication, to sell, release, transfer, share, dis-  
4           seminate, make available, or otherwise cause to be  
5           communicated, such information or contents to a  
6           third party.

7           (14) DOCUMENTARY MATERIAL.—The term  
8           “documentary material” includes the original or any  
9           copy of any book, document, record, report, memo-  
10          randum, paper, communication, tabulation, chart,  
11          logs, electronic files, or other data or data compila-  
12          tions stored in any medium.

13          (15) FEDERAL AGENCY.—The term “Federal  
14          agency” has the meaning given to the term “agen-  
15          cy” in section 3371 of title 5, United States Code.

16          (16) FEDERAL PRIVACY LAWS.—The term  
17          “Federal privacy laws” includes the laws and regula-  
18          tions described in section 502.

19          (17) GOVERNMENT ENTITY.—The term “gov-  
20          ernment entity” means—

21                 (A) a Federal agency;

22                 (B) a State or political subdivision thereof;

23                 (C) or any agency, authority, or instru-  
24          mentality of a State or political subdivision  
25          thereof.



1           (18) INDIVIDUAL.—The term “individual”  
2       means a natural person residing in the United  
3       States.

4           (19) INDIAN TRIBE.—The term “Indian Tribe”  
5       has the meaning given such term in section 4(e) of  
6       the Indian Self-Determination and Education Assist-  
7       ance Act (25 U.S.C. 5304(e)).

8           (20) MAINTAIN.—The term “maintain” means,  
9       with respect to personal information or the contents  
10      of any communication, to store, secure, or otherwise  
11      cause the retention of such information or contents,  
12      or to take actions necessary for storing, securing, or  
13      otherwise causing the retention of such information  
14      or contents.

15          (21) NONPUBLIC INFORMATION.—The term  
16      “nonpublic information” means information that has  
17      not been disclosed in a criminal, civil, or administra-  
18      tive proceeding, in a government investigation, re-  
19      port, or audit, or by the news media or other public  
20      source of information, and that was not obtained in  
21      violation of the law.

22          (22) PERSONAL INFORMATION.—

23              (A) IN GENERAL.—The term “personal in-  
24      formation” means any information maintained  
25      by a covered entity that, on its own or com-

1           bined with other information, is linked or rea-  
2           sonably linkable to a specific individual or a  
3           specific device, including de-identified personal  
4           information and the means to behavioral per-  
5           sonalization created for or linked to a specific  
6           individual.

7           (B) EXCLUSIONS.—The term “personal in-  
8           formation” does not include—

9                   (i) publicly available information  
10           linked to an individual; or

11                   (ii) information derived or inferred  
12           from personal information, if the derived  
13           or inferred information is not linked or  
14           reasonably linkable to a specific individual.

15           (23) PRIVACY HARM.—The term “privacy  
16           harm” means an adverse consequence or a potential  
17           adverse consequence to an individual, a group of in-  
18           dividuals, or society caused from collecting, proc-  
19           essing, maintaining, or disclosing of personal infor-  
20           mation or contents of communications, including—

21                   (A) direct or indirect financial loss or eco-  
22           nomic harm;

23                   (B) physical harm;

24                   (C) psychological harm, including anxiety,  
25           embarrassment, fear, and other trauma;

1 (D) adverse outcomes or decisions with re-  
2 spect to the eligibility of an individual for  
3 rights, benefits, or privileges in employment (in-  
4 cluding hiring, firing, promotion, demotion, and  
5 compensation), credit and insurance (including  
6 denial of an application or obtaining less favor-  
7 able terms), housing, education, professional  
8 certification, or the provision of health care and  
9 related services;

10 (E) stigmatization or reputational harm;

11 (F) price discrimination;

12 (G) adverse consequences that affect the  
13 private life of an individual, including private  
14 family matters and actions and communications  
15 within the home of such individual or a similar  
16 physical, online, or digital location where such  
17 individual has a reasonable expectation that  
18 personal information will not be collected, proc-  
19 essed, or maintained;

20 (H) the chilling of free expression or action  
21 of an individual, a group of individuals, or soci-  
22 ety, due to perceived or actual pervasive and ex-  
23 cessive collecting, processing, disclosing, or  
24 maintaining of personal information or contents  
25 of communications;

1 (I) impairing the autonomy of an indi-  
2 vidual, a group of individuals, or society; and

3 (J) other adverse consequences or potential  
4 adverse consequences, consistent with the provi-  
5 sions of this Act, as determined by the Direc-  
6 tor.

7 (24) PRIVACY-PRESERVING COMPUTING.—

8 (A) IN GENERAL.—The term “privacy-pre-  
9 serving computing” means the collecting, proc-  
10 essing, disclosing, or maintaining of personal  
11 information that has been encrypted or other-  
12 wise rendered unintelligible using a means that  
13 cannot be reversed by a covered entity, or a  
14 covered entity’s service provider, such that—

15 (i) if such personal information could  
16 be rendered intelligible through cooperation  
17 or sharing of cryptographic secrets by mul-  
18 tiple persons, the covered entity has both  
19 technical safeguards and business proc-  
20 esses to prevent such cooperation or shar-  
21 ing;

22 (ii) if such personal information is  
23 rendered intelligible within a hardware  
24 processing unit or other means of per-  
25 forming operations on the information,

1                   there are technical safeguards that, during  
2                   the normal course of operation—

3                               (I) prevent rendering personal in-  
4                               formation intelligible anywhere but  
5                               within the hardware processing unit  
6                               or other means of performing oper-  
7                               ations; and

8                               (II) make the exporting or other-  
9                               wise observing of such intelligible in-  
10                              formation, or the cryptographic secret  
11                              used to protect such information, im-  
12                              possible; and

13                             (iii) if the result of such processing of  
14                             the personal information is also personal  
15                             information, such result must be unintelli-  
16                             gible to the covered entity or service pro-  
17                             vider and protected by privacy-preserving  
18                             computing.

19                             (B) INSUFFICIENT METHODOLOGIES.—The  
20                             Director may determine that a methodology of  
21                             privacy-preserving computing is insufficient for  
22                             the purposes of this definition.

23                             (25) PROCESS.—The term “process” means to  
24                             perform or cause to be performed any operation or  
25                             set of operations on personal information or contents

1 of communication, whether or not by automated  
2 means.

3 (26) PROTECTED CLASS.—The term “protected  
4 class” means the actual or perceived race, color, eth-  
5 nicity, national origin, religion, sex (including sexual  
6 orientation and gender identity or expression), famil-  
7 ial status, or disability of an individual or group of  
8 individuals.

9 (27) PUBLICLY AVAILABLE INFORMATION.—  
10 The term “publicly available information”—

11 (A) means—

12 (i) information that is lawfully made  
13 available from a government entity;

14 (ii) information linked to a public in-  
15 dividual or official that is made publicly  
16 accessible, without restrictions on accessi-  
17 bility other than the general authorization  
18 to access the services used to make the in-  
19 formation accessible;

20 (iii) information of an individual  
21 that—

22 (I) is made publicly accessible by  
23 such individual, without restrictions  
24 on accessibility other than the general  
25 authorization to access the services

1 used to make the information acces-  
2 sible; and

3 (II) such individual has the abil-  
4 ity to delete or change without relying  
5 on a request under section 102 or  
6 103; and

7 (B) does not include—

8 (i) biometric information of an indi-  
9 vidual collected by a covered entity without  
10 the individual's knowledge;

11 (ii) information used for a purpose  
12 that is not compatible with the purpose for  
13 which the information is maintained and  
14 made available in government records;

15 (iii) information obtained from gov-  
16 ernment records for the purpose of selling  
17 such information; or

18 (iv) information used to contact or lo-  
19 cate a private individual either physically  
20 or electronically.

21 (28) REASONABLE MECHANISM.—The term  
22 “reasonable mechanism” means, in the case of a  
23 mechanism for individuals to exercise a right under  
24 title I or interact with a covered entity under title  
25 II, a mechanism that—

1 (A) is equivalent in availability and ease of  
2 use to that of other mechanisms for commu-  
3 nicating or interacting with the covered entity;  
4 and

5 (B) includes an online means of exercising  
6 such right or engaging in such interaction, if  
7 such individuals communicate or interact with  
8 such covered entity through an online medium  
9 or if such covered entity provides information  
10 processing services through a public or widely  
11 available application programming interface (or  
12 similar mechanism).

13 (29) SELL AND SALE.—

14 (A) IN GENERAL.—The terms “sell” and  
15 “sale” mean the disclosing of personal informa-  
16 tion for monetary consideration or for a thing  
17 of value by a covered entity to a third party for  
18 the purposes of processing, maintaining or dis-  
19 closing such personal information at the third-  
20 party’s discretion.

21 (B) EXCLUSIONS.—The terms “sell” and  
22 “sale” do not include—

23 (i) the disclosing of personal informa-  
24 tion of an individual to a third party with  
25 which the individual has a direct relation-



1 ship for purposes of providing a product or  
2 service requested by the individual or oth-  
3 erwise in a manner that is consistent with  
4 an individual's reasonable expectations  
5 considering the context in which the indi-  
6 vidual provided the personal information to  
7 the covered entity;

8 (ii) the disclosing or transfer of per-  
9 sonal information to a subsidiary or an af-  
10 filiate of the covered entity; or

11 (iii) the disclosing or transfer of per-  
12 sonal information to a third party as an  
13 asset that is part of a merger, acquisition,  
14 bankruptcy, or other transaction in which  
15 the third party assumes control of all or  
16 part of the covered entity's assets, unless  
17 personal information makes up the major-  
18 ity of the value of the assets of which the  
19 third party assumes control.

20 (30) SERVICE PROVIDER.—

21 (A) IN GENERAL.—The term “service pro-  
22 vider” means a covered entity that—

23 (i) processes, discloses, or maintains  
24 personal information, where such covered  
25 entity does not process, disclose, or main-

1           tain the personal information other than in  
2           accordance with the directions and on be-  
3           half of another covered entity;

4                 (ii) does not directly collect personal  
5           information from or control the mechanism  
6           for collecting personal information from an  
7           individual;

8                 (iii) does not earn revenue from proc-  
9           essing, maintaining, or disclosing personal  
10          information disclosed to such covered enti-  
11          ty by another covered entity except by pro-  
12          viding contracted services to such other  
13          covered entity;

14                (iv) does not disclose personal infor-  
15          mation to another covered entity unless  
16          such personal information was provided by  
17          such other covered entity or resulted from  
18          maintaining or processing performed on  
19          personal information exclusively provided  
20          by such other covered entity;

21                (v) does not offer services that allow  
22          another covered entity to target specific in-  
23          dividuals using personal information not  
24          provided by such other covered entity;

1 (vi) with respect to personal informa-  
2 tion processed or maintained by such cov-  
3 ered entity on behalf of another covered  
4 entity, assists such other covered entity in  
5 complying with title I, including providing  
6 tools for such other covered entity to com-  
7 ply with such requirements if requested;  
8 and

9 (vii) does not link the personal infor-  
10 mation provided by another covered entity  
11 to personal information from any other  
12 source.

13 (B) TREATMENT.—A covered entity shall  
14 be treated as a service provider under this Act  
15 only to the extent that such covered entity is  
16 acting as a service provider, as defined in sub-  
17 paragraph (A).

18 (31) SIGNIFICANT PRIVACY HARM.—The term  
19 “significant privacy harm” means adverse con-  
20 sequences to an individual arising from the col-  
21 lecting, processing, maintaining, or disclosing of per-  
22 sonal information or contents of communications,  
23 limited to subparagraph (A), (B), or (D) of para-  
24 graph (23).

1           (32) SMALL BUSINESS.—The term “small busi-  
2           ness” means a covered entity that—

3                   (A) does not earn revenue from the sale of  
4           personal information;

5                   (B) earns less than half of annual revenues  
6           from the processing of personal information for  
7           targeted or personalized advertising;

8                   (C) has not, in combination with each sub-  
9           sidiary and affiliate of the service, maintained  
10          personal information of 250,000 or more indi-  
11          viduals for 3 or more of the preceding 12  
12          months;

13                  (D) has fewer than 200 employees; and

14                  (E) received less than \$25,000,000 in  
15          gross revenue in the preceding 12-month pe-  
16          riod.

17           (33) STATE.—The term “State” means each  
18          State of the United States, the District of Columbia,  
19          each commonwealth, territory, or possession of the  
20          United States, and each federally recognized Indian  
21          Tribe.

22           (34) STATE ATTORNEY GENERAL.—The term  
23          “State attorney general” means, with respect to a  
24          State, the attorney general or chief law enforcement  
25          officer of the State, or another official or agency

1 designated by the State to bring civil actions on be-  
2 half of the State or the residents of the State.

3 (35) STATE PRIVACY REGULATOR.—The term  
4 “State privacy regulator” means an agency or in-  
5 strumentality of a State that has the primary pur-  
6 pose of administering, implementing, or enforcing a  
7 privacy law or associated rules or regulations.

8 (36) THIRD PARTY.—The term “third party”  
9 means, with respect to a covered entity, a person—  
10 (A) to which such covered entity disclosed  
11 personal information; and

12 (B) that is not—  
13 (i) such covered entity;  
14 (ii) a subsidiary or corporate affiliate  
15 of such covered entity; or  
16 (iii) a service provider of such covered  
17 entity.

18 (37) USERS.—The term “users” means, with  
19 respect to a product or service, the monthly active  
20 users, subscribers, or customers (or a reasonable  
21 proxy or substitute therefor determined by the Di-  
22 rector) of such product or service.

23 (38) VIOLATION.—The term “violation” means,  
24 except where otherwise specified, any act or omission  
25 that, if proved, would constitute a violation of any

1 provision of this Act or a rule or order issued pursu-  
2 ant to this Act.

3 **SEC. 3. GENERAL PROVISIONS.**

4 (a) RULES OF CONSTRUCTION WITH RESPECT TO  
5 PERSONAL INFORMATION AND INDIVIDUALS.—In this  
6 Act—

7 (1) any reference to information as being of or  
8 belonging to an individual shall be construed to  
9 mean that such information is linked or reasonably  
10 linkable to such individual as described in section  
11 2(21)(A); and

12 (2) any reference to any communication as  
13 being of or belong to an individual shall be con-  
14 strued to mean that such individual is party to such  
15 communication.

16 (b) PROHIBITION ON WAIVERS.—

17 (1) IN GENERAL.—The provisions under this  
18 Act may not be waived. Any agreement purporting  
19 to waive compliance with or modify any provision of  
20 this Act shall be void as contrary to public policy.

21 (2) PROHIBITION ON PREDISPUTE ARBITRATION  
22 AGREEMENTS.—No predispute arbitration agreement  
23 shall be valid or enforceable with respect to any  
24 claims under this Act.

25 (c) JOURNALISM PROTECTION.—

1           (1) IN GENERAL.—Covered entities engaged in  
2       journalism shall not be subject to the obligations im-  
3       posed under this Act to the extent that those obliga-  
4       tions directly infringe on the journalism rather than  
5       the business practices of the covered entity, so long  
6       as the covered entity has technical safeguards and  
7       business processes that prevent the collecting, proc-  
8       essing, maintaining, or disclosing of such personal  
9       information for business practices other than jour-  
10      nalism.

11          (2) JOURNALISM.—The term “journalism” in-  
12      cludes the collecting, maintaining, processing, and  
13      disclosing of personal information about a public in-  
14      dividual or official, or that otherwise concerns mat-  
15      ters of public interest, for dissemination to the pub-  
16      lic.

17          (d) SMALL BUSINESS COMPLIANCE RAMP.—Upon  
18      losing its status as a small business, a covered entity shall  
19      have nine months to comply with provisions of this Act  
20      that a small business is exempt from complying with.

21          (e) PROHIBITION ON COLLECTING, MAINTAINING,  
22      PROCESSING, OR DISCLOSING PERSONAL INFORMA-  
23      TION.—A covered entity may not collect, maintain, proc-  
24      ess, or disclose personal information using a channel of

1 interstate commerce unless such covered entity is in com-  
2 pliance with all requirements of this Act.

3 **SEC. 4. LIMITATION ON DISCLOSING NONREDACTED GOV-**  
4 **ERNMENT RECORDS.**

5 (a) IN GENERAL.—A government entity may not use  
6 a channel of interstate commerce to disclose the personal  
7 information of an individual in a government record with-  
8 out an agreement prohibiting the recipient of such infor-  
9 mation from selling the information without the express  
10 consent of the individual.

11 (b) EXCEPTION.—Notwithstanding subsection (a),  
12 nothing in this section shall prohibit the disclosure of per-  
13 sonal information using a channel of interstate commerce  
14 to another government entity without consent of the indi-  
15 vidual.

16 **SEC. 5. PRIVACY CONSIDERATIONS FOR LEGISLATIVE**  
17 **BRANCH AGENCIES.**

18 (a) GOVERNMENT PUBLISHING OFFICE.—

19 (1) PRIVACY RESPONSIBILITIES OF THE DIREC-  
20 TOR.—

21 (A) IN GENERAL.—Chapter 3 of title 44,  
22 United States Code, is amended by inserting at  
23 the end the following:



1   **“§ 319. Privacy responsibilities of the director of the**  
2                   **government publishing office**

3           “The Director of the Government Publishing Office  
4 shall identify and implement appropriate measures to pre-  
5 vent the disclosure of personal information by the Govern-  
6 ment Publishing Office and to minimize the risk of privacy  
7 harms in its operations.”.

8                   (B) CLERICAL AMENDMENT.—The table of  
9           sections for chapter 3 of title 44, United States  
10          Code, is amended by inserting after the item re-  
11          lating to section 318 the following:

“319. Privacy responsibilities of the director of the government publishing of-  
fice.”.

12                  (2) PRIVACY SAFEGUARDS FOR PUBLISHED  
13          DOCUMENTS.—Section 1701 of title 44, United  
14          States Code, is amended by striking “the publica-  
15          tion.” in the last sentence of the first paragraph and  
16          inserting “the publication, and only after conducting  
17          an appropriate review or implementing other appro-  
18          priate measures to prevent the disclosure of personal  
19          information and minimize the risks of privacy harms  
20          in such publication.”.

21                  (3) PRIVACY SAFEGUARDS IN THE DEPOSITORY  
22          LIBRARY PROGRAM.—Section 1902 of title 44,  
23          United States Code, is amended by inserting at the  
24          end the following: “The Superintendent of Docu-

1       ments shall assess the risks of disclosure of personal  
2       information and related privacy harms in publica-  
3       tions made available to and by depository libraries  
4       and shall implement appropriate measures to mini-  
5       mize such risks, including to the extent necessary by  
6       imposing obligations upon depository libraries.”.

7       (b) LIBRARY OF CONGRESS.—The first paragraph  
8       under the center heading “LIBRARY OF CONGRESS” under  
9       the center heading “LEGISLATIVE” of the Act entitled  
10      “An Act Making appropriations for the legislative, execu-  
11      tive, and judicial expenses of the Government for the fiscal  
12      year ending June thirtieth, eighteen hundred and ninety-  
13      eight, and for other purposes”, approved February 19,  
14      1897 (2 U.S.C. 136), is amended by striking at the end  
15      “Library.” and inserting “Library, including by identi-  
16      fying and implementing appropriate measures to prevent  
17      the disclosure of personal information by the Library and  
18      to minimize the risk of privacy harms in its operations.”.

19      (c) SMITHSONIAN INSTITUTION.—Section 7 of the  
20      Act entitled “An Act to establish the ‘Smithsonian Institu-  
21      tion’ for the increase and diffusion of knowledge among  
22      men”, approved August 10, 1846 (20 U.S.C. 46), is  
23      amended by adding at the end the following: “The Sec-  
24      retary shall assess the risks of disclosure of personal infor-  
25      mation by the institution and related privacy harms and

1 shall implement appropriate measures to minimize such  
2 risks.”.

3 (d) CHIEF ADMINISTRATIVE OFFICER OF THE  
4 HOUSE OF REPRESENTATIVES.—

5 (1) IN GENERAL.—Subchapter III of chapter  
6 55 of title 2, United States Code, is amended by in-  
7 serting at the end the following:

8 **“§ 5549. Privacy responsibilities**

9 “The Chief Administrative Officer of the House of  
10 Representatives shall identify and implement appropriate  
11 measures to prevent the disclosure of personal information  
12 and to minimize the risk of privacy harms in its areas  
13 of operational and financial responsibility.”.

14 (2) CLERICAL AMENDMENT.—The table of sec-  
15 tions for subchapter III of chapter 55 of title 2,  
16 United States Code, is amended by inserting after  
17 the item relating to section 5548 the following:

“5549. Privacy responsibilities.”.

18 **SEC. 6. CRIMINAL PROHIBITION ON DOXXING.**

19 (a) IN GENERAL.—Chapter 41 of title 18, United  
20 States Code, is amended by adding at the end the fol-  
21 lowing:

1 **“§ 881. Disclosing of personal information with the**  
2 **intent to cause harm**

3 “(a) IN GENERAL.—Whoever uses a channel of inter-  
4 state or foreign commerce to knowingly disclose an indi-  
5 vidual’s personal information with the intent—

6 “(1) to threaten, intimidate, or harass any per-  
7 son, incite or facilitate the commission of a crime of  
8 violence against any person, or place any person in  
9 reasonable fear of death or serious bodily injury; or

10 “(2) that the information will be used to threat-  
11 en, intimidate, or harass any person, incite or facili-  
12 tate the commission of a crime of violence against  
13 any person, or place any person in reasonable fear  
14 of death or serious bodily injury,

15 shall be fined under this title or imprisoned not more than  
16 5 years, or both.

17 “(b) DEFINITIONS.—In this section:

18 “(1) CONTENTS.—The term ‘contents’ when  
19 used with respect to communication, has the mean-  
20 ing given such term in section 2510 of title 18,  
21 United States Code.

22 “(2) DISCLOSE.—The term ‘disclose’ means,  
23 with respect to personal information or contents of  
24 communication, to sell, release, transfer, share, dis-  
25 seminate, make available, or otherwise cause to be

1       communicated such information or contents to a  
2       third party.

3           “(3) GOVERNMENT ENTITY.—The term ‘gov-  
4       ernment entity’ means—

5           “(A) a Federal agency (as such term is de-  
6       fined in section 3371 of title 5, United States  
7       Code);

8           “(B) a State or political subdivision there-  
9       of; or

10          “(C) any agency, authority, or instrumen-  
11       tality of a State or political subdivision thereof.

12          “(4) INDIVIDUAL.—The term ‘individual’ means  
13       a natural person residing in the United States.

14          “(5) PERSONAL INFORMATION.—

15          “(A) IN GENERAL.—The term ‘personal in-  
16       formation’ means any information maintained  
17       by a person that, on its own or combined with  
18       other information, is linked or reasonably  
19       linkable to a specific individual.

20          “(B) EXCLUSIONS.—The term ‘personal  
21       information’ does not include—

22           “(i) publicly available information  
23       linked to an individual; or

24           “(ii) information derived or inferred  
25       from personal information, if the derived

1 or inferred information is not linked or  
2 reasonably linkable to a specific individual.

3 “(6) PUBLICLY AVAILABLE INFORMATION.—

4 The term ‘publicly available information’—

5 “(A) means—

6 “(i) information that is lawfully made  
7 available from a government entity;

8 “(ii) information linked to a public in-  
9 dividual or official that is made publicly  
10 accessible, without restrictions on accessi-  
11 bility other than the general authorization  
12 to access the services used to make the in-  
13 formation accessible;

14 “(iii) information of an individual  
15 that—

16 “(I) is made publicly accessible  
17 by such individual, without restric-  
18 tions on accessibility other than the  
19 general authorization to access the  
20 services used to make the information  
21 accessible; and

22 “(II) such individual has the abil-  
23 ity to delete or change; and

24 “(B) does not include—

1 “(i) biometric information of an indi-  
2 vidual collected by a covered entity without  
3 the individual’s knowledge;

4 “(ii) information used for a purpose  
5 that is not compatible with the purpose for  
6 which the information is maintained and  
7 made available in government records;

8 “(iii) information obtained from gov-  
9 ernment records for the purpose of selling  
10 such information; or

11 “(iv) information used to contact or  
12 locate a private individual either physically  
13 or electronically.

14 “(7) STATE.—The term ‘State’ means each  
15 State of the United States, the District of Columbia,  
16 each commonwealth, territory, or possession of the  
17 United States, and each federally recognized Indian  
18 Tribe.”.

19 (b) CLERICAL AMENDMENT.—The table of sections  
20 for chapter 41 of title 18, United States Code, is amended  
21 by inserting after the item relating to section 880 the fol-  
22 lowing:

“881. Disclosing personal information with the intent to cause harm.”.

# 1      **TITLE I—INDIVIDUAL RIGHTS**

## 2      **SEC. 101. RIGHT OF ACCESS.**

3            (a) IN GENERAL.—A covered entity shall make avail-  
4      able a reasonable mechanism by which an individual may  
5      access—

6            (1) the categories of personal information and  
7            contents of communications of such individual that  
8            is maintained by such covered entity, including, in  
9            the case of personal information that such covered  
10          entity did not collect from such individual, how and  
11          from whom such covered entity obtained such per-  
12          sonal information;

13          (2) a list of the third parties, subsidiaries, and  
14          corporate affiliates, to which such covered entity has  
15          disclosed and from which such covered entity has, at  
16          any time on or after the effective date of this Act,  
17          obtained the personal information of such individual;

18          (3) a concise and clear description of the busi-  
19          ness or commercial purposes of such covered enti-  
20          ty—

21                  (A) for collecting, processing, or maintain-  
22                  ing the personal information of such individual;  
23                  and

24                  (B) for disclosing to a third party the per-  
25                  sonal information of such individual; and



1 (4) a list of automated decisionmaking proc-  
2 esses that an individual has a right to request  
3 human review of under section 105 with a concise  
4 and clear description of the implications and in-  
5 tended effects of such process.

6 (b) EXCEPTION FOR PUBLICLY ACCESSIBLE INFOR-  
7 MATION.—A covered entity that makes available informa-  
8 tion required in subsection (a) shall be considered in com-  
9 pliance with such requirements if the covered entity pro-  
10 vides an individual with instructions on how to access a  
11 public posting of such information, including in a privacy  
12 policy, if the instructions are easy and do not require pay-  
13 ment.

14 (c) SMALL BUSINESSES EXCLUDED.—Subsection  
15 (a)(3) does not apply to a small business.

16 **SEC. 102. RIGHT OF CORRECTION.**

17 (a) DISPUTE BY INDIVIDUAL.—A covered entity shall  
18 make available a reasonable mechanism by which an indi-  
19 vidual may dispute the accuracy or completeness of per-  
20 sonal information linked to such individual that is main-  
21 tained by such covered entity if such information is proc-  
22 essed in any way, by such covered entity, a third party  
23 of such covered entity, or a service provider of such cov-  
24 ered entity that may increase reasonably foreseeable sig-  
25 nificant privacy harms.

1 (b) CORRECTION BY COVERED ENTITY.—A covered  
2 entity receiving a dispute under subsection (a) shall—

3 (1) correct or complete (as the case may be) the  
4 disputed information and notify such individual that  
5 the correction or completion has been made; or

6 (2) notify such individual that—

7 (A) the disputed information is correct or  
8 complete;

9 (B) such covered entity lacks sufficient in-  
10 formation to correct or complete the disputed  
11 information; or

12 (C) such covered entity is denying the re-  
13 quest for correction or completion in reliance on  
14 an exemption or exception provided by section  
15 109(g).

16 (c) SMALL BUSINESSES EXCLUDED.—This section  
17 does not apply to a small business.

18 **SEC. 103. RIGHT OF DELETION.**

19 (a) REQUEST BY INDIVIDUAL.—A covered entity  
20 shall make available a reasonable mechanism by which an  
21 individual may request the deletion of personal informa-  
22 tion and contents of communications of such individual  
23 maintained by such covered entity, including any such in-  
24 formation that such covered entity acquired from a third

1 party or inferred from other information maintained by  
2 such covered entity.

3 (b) DELETION BY COVERED ENTITY.—A covered en-  
4 tity receiving a request for deletion under subsection (a)  
5 shall—

6 (1) delete such information and notify such in-  
7 dividual that such information has been deleted; or

8 (2) notify such individual that such covered en-  
9 tity is denying the request for deletion in reliance on  
10 an exemption or exception provided by section  
11 109(g).

12 **SEC. 104. RIGHT OF PORTABILITY.**

13 (a) DETERMINATION OF PORTABLE CATEGORIES.—

14 (1) ANNUAL DETERMINATION.—Not less fre-  
15 quently than once per calendar year, the Director  
16 shall—

17 (A) establish categories of products and  
18 services offered by covered entities, based on  
19 similarities in the products and services;

20 (B) determine which categories established  
21 under subparagraph (A) are portable categories;  
22 and

23 (C) publish in the Federal Register a list  
24 of portable categories determined under sub-  
25 paragraph (B).

1 (2) OPPORTUNITY FOR PUBLIC COMMENT.—Be-  
2 fore publishing the final list under paragraph (1)(C),  
3 the Director shall—

4 (A) publish a draft of such list in the Fed-  
5 eral Register; and

6 (B) provide an opportunity for public com-  
7 ment on such draft list.

8 (b) EXERCISE OF RIGHT.—

9 (1) IN GENERAL.—A covered entity that offers  
10 a product or service in a portable category and that  
11 maintains personal information or the contents of  
12 any communications of an individual shall make  
13 available to such individual a reasonable mechanism  
14 by which such individual may—

15 (A) download, in a format that is struc-  
16 tured, commonly used, and machine-readable—

17 (i) any such personal information that  
18 such individual has provided to such cov-  
19 ered entity, with the option to download  
20 such information by category that is acces-  
21 sible under section 101; and

22 (ii) the contents of any such commu-  
23 nications; and

24 (B) using a real-time application program-  
25 ming interface, or similar mechanism, transmit

1 all such personal information (whether or not  
2 provided to such covered entity by such indi-  
3 vidual) and the contents of any such commu-  
4 nication from such covered entity to another  
5 covered entity in accordance with subsection  
6 (c).

7 (2) REQUIREMENTS FOR APPLICATION PRO-  
8 GRAMMING INTERFACE.—The application program-  
9 ming interface, or similar mechanism, required by  
10 paragraph (1)(B) shall—

11 (A) be publicly documented;

12 (B) allow the option of obtaining any per-  
13 sonal information of an individual that the indi-  
14 vidual has provided to the covered entity, if  
15 such information is accessible under section  
16 101;

17 (C) include a publicly available, fully func-  
18 tional test version for development purposes;  
19 and

20 (D) be of similar quality to mechanisms  
21 used internally by the covered entity.

22 (c) REQUIREMENTS FOR ACCESS TO AN APPLICATION  
23 PROGRAMMING INTERFACE.—

24 (1) ACCESS.—Except as provided in paragraph

25 (2)(A), a covered entity shall provide access to the

1 application programming interface or similar mecha-  
2 nism required by subsection (b)(1)(B) upon the re-  
3 quest of another covered entity if the requesting cov-  
4 ered entity has self-certified, using the procedures  
5 established by the Director under paragraph (3)(A),  
6 that such requesting covered entity—

7 (A) is a covered entity;

8 (B) can have personal information dis-  
9 closed to it under section 204;

10 (C) is, at the time of the self-certification,  
11 in compliance with all applicable requirements  
12 of this Act (including provisions a small busi-  
13 ness is otherwise exempt from complying with);

14 (D) will continue to comply with all re-  
15 quirements of this Act; and

16 (E) will only use such application program-  
17 ming interface or similar mechanism at the ex-  
18 press request of an individual.

19 (2) DENIAL OF ACCESS.—

20 (A) IN GENERAL.—A covered entity may  
21 deny access to the application programming  
22 interface or similar mechanism required by sub-  
23 section (b)(1)(B) if such covered entity has an  
24 objective, reasonable belief that the requesting

1 covered entity has failed to meet the require-  
2 ments for self-certification under paragraph (1).

3 (B) REVIEW.—In accordance with the pro-  
4 cedures established under paragraph (3)(B), a  
5 covered entity the request of which is denied  
6 under subparagraph (A) may petition the Di-  
7 rector for review of the denial. If the Director  
8 finds that such denial is unreasonable, the Di-  
9 rector shall impose a penalty, to be established  
10 in such procedures, on the covered entity that  
11 denied the request.

12 (3) CERTIFICATION AND REVIEW PROCE-  
13 DURES.—The Director shall establish—

14 (A) procedures for a covered entity to self-  
15 certify under paragraph (1); and

16 (B) procedures for the review of petitions  
17 under paragraph (2)(B), including penalties for  
18 unreasonable denials.

19 (d) SMALL BUSINESSES EXCLUDED.—This section  
20 does not apply to a small business.

21 (e) PORTABLE CATEGORY DEFINED.—In this sec-  
22 tion, the term “portable category” means a category of  
23 products and services established by the Director under  
24 subsection (a)(1)(A)—

1 (1) for which the sum obtained by adding the  
2 number of users or estimated users of each product  
3 or service in such category is greater than  
4 10,000,000; and

5 (2) that—

6 (A) has an estimated Herfindahl-  
7 Hirschman Index of 2,000 or greater;

8 (B) has 3 or fewer covered entities offering  
9 products and services in such category; or

10 (C) the Director otherwise determines that  
11 a category would benefit from encouraging in-  
12 creased competition.

13 **SEC. 105. RIGHT TO HUMAN REVIEW OF AUTOMATED DECI-**  
14 **SIONS.**

15 For any decision by a covered entity based solely on  
16 automated processing of personal information of an indi-  
17 vidual, if such processing materially increases reasonably  
18 foreseeable significant privacy harms for such individual,  
19 such covered entity shall—

20 (1) inform such individual of what personal in-  
21 formation is being or may be used for such decision;

22 (2) make available a reasonable mechanism by  
23 which such individual may request human review of  
24 such decision, upon request or in a publicly acces-  
25 sible location; and



1           (3) if such individual requests such a review,  
2       conduct such review within a reasonable amount of  
3       time after such request.

4 **SEC. 106. RIGHT TO INDIVIDUAL AUTONOMY.**

5       (a) IN GENERAL.—A covered entity shall not collect,  
6       process, maintain, or disclose an individual’s personal in-  
7       formation to—

8           (1) create, improve upon, or maintain;

9           (2) process with; or

10          (3) otherwise link an individual with;

11   an algorithm, model, or other means designed for behav-  
12   ioral personalization, without the affirmative express con-  
13   sent of that individual.

14       (b) CONSENT.—A covered entity must obtain express  
15   affirmative consent from an individual before it may pro-  
16   vide a behaviorally personalized version of a product or  
17   service, and not less than every calendar year thereafter.  
18   Where consent is denied, a covered entity must provide  
19   the product or service without behavioral personalization.

20       (c) EXCEPTIONS TO PROVIDING PRODUCT OR SERV-  
21   ICE.—

22           (1) Where the offering of a substantially similar  
23       product or service without behavioral personalization  
24       is infeasible, a covered entity shall provide, to the  
25       greatest extent feasible, a core aspect or part of the

1 product or service that can be offered without behav-  
2 ioral personalization.

3 (2) Where no core aspect or part of the product  
4 or service can function in a substantially similar  
5 function without behavioral personalization, a cov-  
6 ered entity may deny providing an individual use of  
7 such product or service if such individual does not  
8 consent to behavioral personalization as required in  
9 subsection (a).

10 (d) EXCEPTION TO BEHAVIORAL PROCESSING.—Not-  
11 withstanding subsections (a) and (b), a covered entity may  
12 process personal information to create or operate behav-  
13 ioral personalization algorithms, models, or other mecha-  
14 nisms for the purpose of increasing the usability of the  
15 product or service provided by a covered entity that—

16 (1) are built using aggregated personal infor-  
17 mation that is representative of all the personal in-  
18 formation the covered entity maintains; and

19 (2) have an output that is both uniform across  
20 the individuals that use the product or service and  
21 independent of a specific individual’s inherent or be-  
22 havioral characteristics.

23 (e) USABILITY.—The term “usability” as used in  
24 subsection (d) does not include optimizations or other al-  
25 terations to the product or service that are made with the

1 primary purpose of increasing the amount of time an indi-  
2 vidual engages with or uses the product or service, unless  
3 such increase benefits the individual.

4 (f) **SMALL BUSINESSES EXCLUDED.**—This section  
5 does not apply to a small business.

6 **SEC. 107. RIGHT TO BE INFORMED.**

7 A covered entity that collects personal information of  
8 an individual with whom such covered entity does not have  
9 an existing relationship (as of the time of the collecting),  
10 if such personal information includes contact information,  
11 shall notify such individual within 30 days, in writing if  
12 possible and at no charge to the individual, that such cov-  
13 ered entity has collected the personal information of such  
14 individual.

15 **SEC. 108. RIGHT TO IMPERMANENCE.**

16 (a) **LIMITATION ON MAINTAINING OF PERSONAL IN-**  
17 **FORMATION.**—A covered entity shall not maintain per-  
18 sonal information for more time than expressly consented  
19 to by an individual whose personal information is being  
20 maintained.

21 (b) **CONSENT.**—A covered entity must obtain express  
22 affirmative consent from an individual before maintaining  
23 the personal information of such individual for any dura-  
24 tion. Such consent may be obtained for categories of per-  
25 sonal information and shall give an individual options to

1 affirmatively choose granting a covered entity consent for  
2 various durations, at least including—

3 (1) for no longer than needed to complete the  
4 specific request or transaction (including a reason-  
5 able estimate of such duration by the covered enti-  
6 ty);

7 (2) until consent is revoked; and

8 (3) one or more additional durations based on  
9 reasonable expectations and norms for maintaining  
10 the category of personal information.

11 (c) EXCEPTION FOR IMPLIED CONSENT.—Where the  
12 long-term maintaining of personal information is, on its  
13 face, obvious and a core feature of the product or service  
14 at the request of the individual, and the personal informa-  
15 tion is maintained only to provide such product or service,  
16 subsections (a) and (b) shall not apply.

17 **SEC. 109. EXEMPTIONS, EXCEPTIONS, FEES, TIMELINES,**  
18 **AND RULES OF CONSTRUCTION FOR RIGHTS**  
19 **UNDER THIS TITLE.**

20 (a) EXEMPTIONS FOR PERSONAL INFORMATION FOR  
21 PARTICULAR PURPOSES.—

22 (1) IN GENERAL.—This title does not apply  
23 with respect to personal information that is col-  
24 lected, processed, maintained, or disclosed for any of  
25 the following purposes (or a combination of such

1 purposes), where a covered entity has technical safe-  
2 guards and business processes that limit collecting,  
3 processing, maintaining, or disclosing of such per-  
4 sonal information to the following purposes:

5 (A) Detecting, responding to, or preventing  
6 security incidents or threats.

7 (B) Protecting against malicious, decep-  
8 tive, fraudulent, or illegal activity.

9 (C) A good faith response to, or compli-  
10 ance with, a valid subpoena, court order, or  
11 warrant (including a subpoena and court order  
12 obtained by an entity that is not a government  
13 entity) or otherwise providing information as  
14 required by law.

15 (D) Protecting a legally recognized privi-  
16 lege or other legal right.

17 (E) Protecting public safety.

18 (F) Collecting, processing, or maintaining  
19 by an employer pursuant to an employer-em-  
20 ployee relationship of records about employees  
21 or employment status, except—

22 (i) where the information would not  
23 be reasonably expected to be collected in  
24 the context of an employee's regular du-  
25 ties; or

1 (ii) was disclosed to the employer by  
2 a third party.

3 (G) Preventing prospective abuses of a  
4 service by an individual whose account has been  
5 previously terminated.

6 (H) Routing a communication through a  
7 communications network or resolving the loca-  
8 tion of a host or client on a communications  
9 network.

10 (I) Providing transparency in advertising  
11 or origination of user-generated content.

12 (2) REIDENTIFICATION.—Where compliance  
13 with this title would require the reidentification of  
14 de-identified personal information, and the covered  
15 entity does not already maintain the information  
16 necessary for such reidentification, the covered enti-  
17 ty shall be exempt from such compliance, except for  
18 requirements under section 106.

19 (3) DISCLOSING.—A covered entity relying on  
20 an exemption under paragraph (1) with respect to  
21 personal information shall disclose in the privacy  
22 policy maintained by such entity under section  
23 211—

1 (A) the reason for which such information  
2 is collected, processed, maintained, or disclosed;  
3 and

4 (B) a description of the rights provided by  
5 this title that are not available with respect to  
6 such personal information by reason of such ex-  
7 emption.

8 (b) EXCEPTIONS FOR PARTICULAR REQUESTS.—

9 (1) IN GENERAL.—A covered entity may deny  
10 the request of an individual under this title if—

11 (A) such covered entity cannot confirm the  
12 identity of such individual;

13 (B) such covered entity determines that  
14 granting the request of such individual would  
15 create a legitimate risk to the privacy, security,  
16 safety, or other rights of another individual;

17 (C) such covered entity determines that  
18 granting the request of such individual would  
19 create a legitimate risk to free expression; or

20 (D) the personal information requested to  
21 be corrected under section 102 or deleted under  
22 section 103—

23 (i) is necessary to the completion of a  
24 transaction initiated before such request

1                   was made or the performance of a contract  
2                   entered into before such request was made;  
3                   (ii) was collected specifically for the  
4                   completion of such transaction or the per-  
5                   formance of such contract; and  
6                   (iii) would undermine the integrity of  
7                   a legally significant transaction.

8                   (2) LIMITATIONS ON REQUESTS FOR ADDI-  
9                   TIONAL INFORMATION TO CONFIRM IDENTITY.—A  
10                  covered entity may not deny a request of an indi-  
11                  vidual under paragraph (1)(A) on the basis of the  
12                  refusal of such individual to provide additional per-  
13                  sonal information to such covered entity to confirm  
14                  the identity of such individual—

15                  (A) if the identity of such individual can  
16                  reasonably be confirmed using personal infor-  
17                  mation of such individual that such covered en-  
18                  tity (as of the time of the request) already  
19                  maintains; or

20                  (B) if such individual has an existing rela-  
21                  tionship (as of the time of the request) with  
22                  such covered entity, such individual has con-  
23                  firmed the identity of such individual to such  
24                  covered entity in the same manner as for other  
25                  transactions of a similar sensitivity.



1 (c) EXEMPTION FOR SERVICE PROVIDERS.—This  
2 title does not apply to a service provider.

3 (d) EXEMPTION FOR PRIVACY-PRESERVING COM-  
4 PUTING.—Except for sections 101, 105, and 106, this title  
5 does not apply to personal information secured using pri-  
6 vacy-preserving computing.

7 (e) TIMELINE FOR COMPLYING WITH A REQUEST.—  
8 Without undue delay but not longer than 30 days after  
9 the request, a covered entity that receives a request under  
10 this title must—

11 (1) comply with such request; or

12 (2) inform such individual of the reason for de-  
13 nying such request, as allowed under subsection (a)  
14 or (b).

15 (f) FEES PROHIBITED.—

16 (1) IN GENERAL.—Except as provided in para-  
17 graph (2), a covered entity may not charge a fee to  
18 an individual for a request made under this title.

19 (2) UNFOUNDED OR EXCESSIVE REQUESTS.—If  
20 a request under this title is unfounded or excessive,  
21 a covered entity may charge a reasonable fee that  
22 reflects the estimated administrative costs of com-  
23 plying with such request.

1           (3) AGENCY NOTICE.—If a covered entity plans  
2           to charge fee under paragraph (2), it must notify  
3           the Agency at least 7 days before charging such fee.

4           (4) AGENCY REVIEW.—The Director may reject  
5           any fee that a covered entity plans to charge for a  
6           request made under this title if the Agency finds—

7                   (A) such fee to be unreasonable relative to  
8                   reasonable administrative costs of complying  
9                   with a request under this title; or

10                   (B) such request is not unfounded or ex-  
11                   cessive.

12           (g) RULES OF CONSTRUCTION.—Nothing in this title  
13           shall be construed to require a covered entity to—

14                   (1) take an action that would convert informa-  
15                   tion that is not personal information into personal  
16                   information;

17                   (2) collect or maintain personal information or  
18                   contents of communication that the covered entity  
19                   would otherwise not maintain (including record of an  
20                   individual exercising rights under this title); or

21                   (3) maintain personal information or contents  
22                   of communication longer than the covered entity  
23                   would otherwise maintain such personal information.

24           (h) REGULATIONS.—The Director shall promulgate  
25           regulations to implement this section.

1 **TITLE II—REQUIREMENTS FOR**  
2 **COVERED ENTITIES, SERVICE**  
3 **PROVIDERS, AND THIRD PAR-**  
4 **TIES**

5 **SEC. 201. MINIMIZATION.**

6 (a) **ARTICULATED BASIS.**—A covered entity shall  
7 have a reasonable, articulated basis for collecting, proc-  
8 essing, maintaining, and disclosing of personal informa-  
9 tion that takes into account the reasonable business needs  
10 of the covered entity and minimum amount of personal  
11 information necessary for providing the service, balanced  
12 with the intrusion on the privacy of, potential privacy  
13 harms to, and reasonable expectations of individuals to  
14 whom the personal information relates.

15 (b) **MINIMIZATION OF COLLECTING, PROCESSING,**  
16 **MAINTAINING, AND DISCLOSING.**—

17 (1) **COLLECTING.**—A covered entity may not  
18 collect more personal information than is reasonably  
19 needed to provide a product or service that an indi-  
20 vidual has requested.

21 (2) **PROCESSING.**—A covered entity may not  
22 process personal information for a purpose other  
23 than the purpose for which such information was  
24 originally collected from the individual or in the case  
25 of a service provider, a purpose other than that

1       which is in accordance with the directions of a cov-  
2       ered entity.

3           (3) MAINTAINING.—A covered entity may not  
4       maintain personal information once such information  
5       is no longer needed for the purpose for which such  
6       information was originally collected from the indi-  
7       vidual or in the case of a service provider, a purpose  
8       other than that which is in accordance with the di-  
9       rections of a covered entity.

10          (4) DISCLOSING.—A covered entity may not  
11       disclose personal information for a purpose other  
12       than the purpose for which such information was  
13       originally collected from the individual or in the case  
14       of a service provider, a purpose other than that  
15       which is in accordance with the directions of a cov-  
16       ered entity.

17       (c) ANCILLARY COLLECTING, PROCESSING, MAIN-  
18       TAINING, AND DISCLOSING.—Notwithstanding subsection  
19       (b), a covered entity may collect, process, disclose, or  
20       maintain personal information beyond limitations under  
21       subsection (b) only if such covered entity complies with  
22       this subsection.

23          (1) NO NOTICE OR CONSENT REQUIRED.—A  
24       covered entity may collect, process, or maintain per-  
25       sonal information without additional notice or con-

1 sent if the purpose for such collecting, processing, or  
2 maintaining is substantially similar to the type of  
3 personal information and purpose for which such  
4 personal information was originally collected and  
5 such ancillary collecting, processing, or maintaining  
6 will not result in additional or increased privacy  
7 harms.

8 (2) NOTICE REQUIRED.—A covered entity shall  
9 provide notice of ancillary collecting, processing,  
10 maintaining, or disclosing of personal information in  
11 the case of one, but not more than one, of the fol-  
12 lowing instances:

13 (A) Such ancillary collecting, processing,  
14 maintaining, or disclosing may result in addi-  
15 tional or increased privacy harms (but not in-  
16 creased significant privacy harms), and is sub-  
17 stantially similar to the purpose for which such  
18 personal information was originally collected.

19 (B) Such ancillary collecting, processing,  
20 maintaining, or disclosing is not substantially  
21 similar to the purpose for which such personal  
22 information was originally collected, but will not  
23 result in additional or increased privacy harms.

24 (C) Such ancillary collecting, processing,  
25 maintaining, or disclosing may result in addi-

1           tional or increased privacy harms (but not in-  
2           creased significant privacy harms) and the pur-  
3           pose is not substantially similar to the purpose  
4           for which such personal information was origi-  
5           nally collected, so long as the personal informa-  
6           tion is secured using privacy preserving com-  
7           puting.

8           (3) NOTICE AND CONSENT REQUIRED.—For  
9           scenarios not covered under paragraph (1) or (2),  
10          and notwithstanding sections 208(b)(2) and (3), a  
11          covered entity shall provide notice of and obtain con-  
12          sent for ancillary collecting, processing, maintaining,  
13          or disclosing of personal information.

14          (d) SUBSTITUTION.—In cases in which personal in-  
15          formation can be replaced with artificial personal informa-  
16          tion, personal information that has been de-identified, or  
17          the random personal information of one or more individ-  
18          uals without substantially reducing the utility of the data  
19          or requiring an unreasonable amount of effort, such a re-  
20          placement shall take place.

21   **SEC. 202. MINIMIZATION AND RECORDS OF ACCESS BY EM-**  
22                           **PLOYEES AND CONTRACTORS.**

23          (a) MINIMIZATION.—A covered entity shall restrict  
24          access to personal information and contents of commu-  
25          nications by the employees or contractors of such covered

1 entity based on an articulated balance between the poten-  
2 tial for privacy harm, reasonable expectations of individ-  
3 uals to whom the personal information relates, and reason-  
4 able business needs.

5 (b) RECORDS OF ACCESS.—

6 (1) IN GENERAL.—A covered entity shall main-  
7 tain records identifying each instance in which an  
8 employee or a contractor of such covered entity ac-  
9 cesses personal information or contents of commu-  
10 nications if disclosing such personal information or  
11 contents of communication, or a data breach or  
12 data-sharing abuse involving such personal informa-  
13 tion or contents of communication, may foreseeably  
14 result in increased privacy harms.

15 (2) INFORMATION REQUIRED.—The records re-  
16 quired by paragraph (1) shall include the following:

17 (A) A unique identifier for the employee or  
18 contractor accessing personal information or  
19 contents of communications.

20 (B) The date and time of access.

21 (C) The fields of information accessed.

22 (D) The individuals whose personal infor-  
23 mation was accessed or the contents of whose  
24 communications were accessed.

1 (3) SMALL BUSINESSES EXCLUDED.—This sub-  
2 section does not apply to a small business.

3 **SEC. 203. PROHIBITIONS ON DISCLOSING OF PERSONAL IN-**  
4 **FORMATION.**

5 (a) CONSENT FOR DISCLOSING REQUIRED.—

6 (1) IN GENERAL.—A covered entity may not in-  
7 tentiously disclose personal information unless the  
8 covered entity obtains consent of the individual  
9 whose personal information is being disclosed for  
10 each category of third party to which such personal  
11 information will be disclosed. Such covered entity  
12 must also provide such individual with notice of—

13 (A) each category of third party;

14 (B) the personal information to be dis-  
15 closed; and

16 (C) a concise and clear description of the  
17 business or commercial purpose for disclosing  
18 such personal information.

19 (2) ADDITIONAL REQUIREMENTS FOR SALE OF  
20 PERSONAL INFORMATION.—

21 (A) IN GENERAL.—A covered entity may  
22 not intentionally sell personal information un-  
23 less the covered entity—



1 (i) obtains the consent required by  
2 paragraph (1) for disclosing such personal  
3 information; and

4 (ii) provides the individual to whom  
5 such personal information relates with the  
6 identity of the specific third party to which  
7 such personal information will be disclosed.

8 (B) DISCLOSING SERVICES.—Subpara-  
9 graph (A) shall not apply to a covered entity in  
10 a case in which an individual is directing the  
11 covered entity to disclose the personal informa-  
12 tion of such individual for the sole purpose of  
13 procuring goods or services, or offers for goods  
14 or services, for such individual, if there is a rea-  
15 sonable mechanism for the individual to with-  
16 draw consent.

17 (3) REQUIREMENT TO INCLUDE ORIGINAL PUR-  
18 POSE OF COLLECTING.—A covered entity may not  
19 intentionally disclose personal information without  
20 including the purpose for which the personal infor-  
21 mation was originally collected.

22 (4) EXCEPTION FOR PRIVACY-PRESERVING  
23 COMPUTING.—Notwithstanding paragraph (1), con-  
24 sent is not required for disclosing (not including sell-

1       ing) personal information secured using privacy pre-  
2       serving computing.

3           (5) EXCEPTION FOR DE-IDENTIFIED PERSONAL  
4       INFORMATION.—Notwithstanding paragraph (1),  
5       consent is not required for disclosing (not including  
6       selling) de-identified personal information where the  
7       disclosed personal information is limited to the nar-  
8       rowest possible scope likely to yield the intended  
9       benefit and contractual obligations are in place that  
10      prohibit—

11           (A) re-identification of the disclosed per-  
12      sonal information; and

13           (B) the processing of additional personal  
14      information in combination with the disclosed  
15      personal information that would allow for the  
16      reidentification of the disclosed personal infor-  
17      mation.

18      (b) DISCLOSING FOR ADVERTISING OR MARKETING  
19      PURPOSES.—

20           (1) IN GENERAL.—A covered entity may not in-  
21      tentionally disclose for advertising or marketing pur-  
22      poses a unique identifier or any other personal infor-  
23      mation that would allow information disclosed to be  
24      linked to information relating to the same individual  
25      or device disclosed in the past.

1           (2) TREATMENT OF CERTAIN TYPES OF INFOR-  
2           MATION.—Disclosing personal information or con-  
3           tents of communication for advertising or marketing  
4           purposes may not be treated as violating paragraph  
5           (1) by reason of including any or all of the following:

6                   (A) Internet Protocol addresses truncated  
7                   to no more than the first 24 bits for Internet  
8                   Protocol version 4 and the first 48 bits for  
9                   Internet Protocol version 6, or for a successor  
10                  protocol truncated to limit the precision of the  
11                  identifier to a network address of the internet  
12                  access provider.

13                  (B) Geolocation information truncated to  
14                  allow no more than the equivalent of two dec-  
15                  imal degrees of precision at the equator or  
16                  prime meridian, or an equivalent precision in  
17                  another geolocation standard.

18                  (C) A general description of a device,  
19                  browser, or operating system, or any combina-  
20                  tion thereof.

21                  (D) An identifier that is unique to a dislo-  
22                  sure.

1 **SEC. 204. DISCLOSING TO ENTITIES NOT SUBJECT TO**  
2 **UNITED STATES JURISDICTION OR NOT COM-**  
3 **PLIANT WITH THIS ACT.**

4 (a) PROHIBITION.—A covered entity may not inten-  
5 tionally disclose personal information to any entity that—

6 (1) is not subject to the jurisdiction of the  
7 United States; or

8 (2) is not in compliance with all requirements  
9 of this Act.

10 (b) EXCEPTION.—Notwithstanding subsection (a), a  
11 covered entity may disclose personal information where  
12 that personal information is limited to an identifier cre-  
13 ated primarily for the purpose of sending or receiving elec-  
14 tronic communications and the sole purpose of disclosing  
15 is to send or receive an electronic communication at the  
16 request of the individual whose personal information is  
17 being disclosed.

18 (c) SAFE HARBORS FOR DISCLOSING.—Notwith-  
19 standing subsection (a), a covered entity may disclose per-  
20 sonal information to another covered entity (the receiving  
21 covered entity) that is not subject to the jurisdiction of  
22 the United States if either—

23 (1) the receiving covered entity has entered into  
24 an agreement, as described in subsection (e), with  
25 the Agency, and—

1 (A) the covered entity has a reasonable be-  
2 lief that the receiving covered entity is suffi-  
3 ciently solvent to compensate victims or pay  
4 fines for violations of this Act;

5 (B) a contract between the covered entity  
6 and receiving covered entity requires that the  
7 receiving covered entity complies with this Act,  
8 and the covered entity has reason to believe the  
9 receiving covered entity is compliant with this  
10 Act; and

11 (C) a contract between the covered entity  
12 and the receiving covered entity prohibits the  
13 receiving covered entity from using the dis-  
14 closed personal information for any purpose  
15 other than provided in the contract; or

16 (2) the covered entity has—

17 (A) entered into an agreement with the re-  
18 ceiving covered entity that—

19 (i) requires the receiving covered enti-  
20 ty to comply with this Act;

21 (ii) prohibits the receiving covered en-  
22 tity from using the disclosed personal in-  
23 formation for any purpose other than pro-  
24 vided in the contract;

1 (iii) requires the receiving covered en-  
2 tity to indemnify the covered entity against  
3 violations of this Act committed by the re-  
4 ceiving covered entity for any amount the  
5 covered entity is unable to pay of a judg-  
6 ment for such violation;

7 (iv) grants the covered entity the au-  
8 thority to audit, including physical access  
9 to electronic devices and data, the receiving  
10 covered entity's compliance with this Act  
11 and the contract; and

12 (v) requires the receiving covered enti-  
13 ty to assist the covered entity in respond-  
14 ing to and complying with any court or-  
15 ders, Agency orders, or the exercising of  
16 an individual's rights under this Act;

17 (B) actual knowledge that the receiving  
18 covered entity is in compliance with this Act  
19 and not using personal information contrary to  
20 their agreement;

21 (C) actual knowledge that the receiving  
22 covered entity is sufficiently solvent to com-  
23 pensate victims or pay fines for violations of  
24 this Act;

1 (D) an auditing and compliance program  
2 to ensure the receiving covered entity's contin-  
3 ued compliance with this Act and contract  
4 terms;

5 (E) filed with the Agency the terms of said  
6 contract, proof of its actual knowledge of the  
7 receiving covered entity's compliance with this  
8 Act and contract terms, and documents detail-  
9 ing its auditing and compliance program for ap-  
10 proval and publication by the Agency; and

11 (F) entered into an agreement with the  
12 Agency where the covered entity agrees to ac-  
13 cept, respond to, or comply with a court order,  
14 Agency order, or request by an individual re-  
15 garding actions taken by the receiving covered  
16 entity with respect to covered information it has  
17 disclosed.

18 (d) LIABILITY FOR VIOLATION BY RECEIVING COV-  
19 ERED ENTITY; FAILURE TO REPORT.—For the purposes  
20 of subsection (c)(2), the covered entity shall be jointly lia-  
21 ble for a violation of this Act by the receiving covered enti-  
22 ty regarding the personal information the covered entity  
23 disclosed, except where the covered entity was the first to  
24 notify the Agency of the violation, in which case, it shall  
25 be severally liable. Where the covered entity should reason-

1 ably have known of a violation of this Act by the receiving  
2 covered entity and fails to disclose the violation to the  
3 Agency, each day of continuance of the failure to report  
4 such violation shall be treated as a separate violation.

5 (e) AGENCY AGREEMENTS.—Upon the request of a  
6 covered entity not subject to the jurisdiction of the United  
7 States, the Agency shall enter into an agreement with the  
8 covered entity that includes, but is not limited to, the fol-  
9 lowing conditions:

10 (1) The principal place of business for the cov-  
11 ered entity must be in a country that allows for the  
12 domestication of a United States court decision for  
13 civil fines payable to a government entity and in-  
14 junctive relief. Where a foreign court refuses to en-  
15 force a United States court decision under this Act,  
16 the agreement, and all other agreements with cov-  
17 ered entities with a principal place of business in the  
18 same jurisdiction, shall be void.

19 (2) The covered entity agrees to comply with  
20 this Act.

21 (3) The covered entity agrees to be subject to  
22 this Act with choice of venue being a United States  
23 court.



1           (4) The covered entity agrees to comply with  
2       Agency investigative requests or orders, and United  
3       States court orders or decisions under this Act.

4           (5) The covered entity consents to United  
5       States Federal court personal jurisdiction for the  
6       sole purpose of enforcing this Act.

7           (6) Where enforcement of the decision requires  
8       the use of a foreign court, the covered entity agrees  
9       to pay reasonable attorney fees necessary to enforce  
10      the judgment.

11          (7) A default judgment, failure to comply with  
12      Agency investigative requests or orders, or failure to  
13      comply with United States court orders or decisions  
14      shall result in the immediate termination of the  
15      agreement.

16      (f) RULE OF CONSTRUCTION AGAINST DATA LOCAL-  
17      IZATION.—Nothing in this section shall be construed to  
18      require the localization of processing or maintaining per-  
19      sonal information by a covered entity to within the United  
20      States, or limit internal disclosing of personal information  
21      within a covered entity or to subsidiary or corporate affil-  
22      iate of such covered entity, regardless of the country in  
23      which the covered entity will process, disclose, or maintain  
24      that personal information.

1 **SEC. 205. PROHIBITION ON REIDENTIFICATION.**

2 (a) IN GENERAL.—Except as required under title I,  
3 a covered entity shall not use personal information col-  
4 lected from an individual, acquired from a third party, or  
5 acquired from a publicly available information to reiden-  
6 tify an individual from de-identified information.

7 (b) THIRD-PARTY PROHIBITION.—A covered entity  
8 that discloses de-identified information to a third party  
9 shall prohibit such third party from reidentifying an indi-  
10 vidual using such de-identified information.

11 (c) EXCEPTION.—Subsection (a) shall not apply to  
12 qualified research entities, as determined by the Director,  
13 conducting research not for commercial purposes.

14 **SEC. 206. RESTRICTIONS ON COLLECTING, PROCESSING,**  
15 **MAINTAINING, AND DISCLOSING CONTENTS**  
16 **OF COMMUNICATIONS.**

17 (a) IN GENERAL.—A covered entity may not collect,  
18 process, maintain, or disclose the contents of any commu-  
19 nication, regardless of whether the sender or intended re-  
20 cipient of the communication is an individual, other per-  
21 son, or an electronic device, for any purpose other than—

22 (1) transmitting or displaying the communica-  
23 tion to any intended recipient or the original sender,  
24 or maintaining such communications for such pur-  
25 poses;

1           (2) detecting, responding to, or preventing secu-  
2       rity incidents or threats;

3           (3) providing services to assist in the drafting  
4       or creation of the content of a communication;

5           (4) processing expressly requested by the sender  
6       or intended recipient, if the sender or intended re-  
7       cipient can terminate such processing using a rea-  
8       sonable mechanism;

9           (5) disclosing otherwise required by law;

10          (6) filtering a communication where primary  
11       purpose of the communication is the commercial ad-  
12       vertisement or promotion of a commercial product or  
13       service of a covered entity; or

14          (7) detecting or enforcing an abuse or violation  
15       of the terms of service of the covered entity that  
16       would result in either a temporary or permanent ban  
17       from using the service.

18       (b) INTENDED RECIPIENT.—A covered entity is not  
19       considered an intended recipient of a communication, or  
20       any communication used in the creation of the content of  
21       said communication, where—

22           (1) at least one intended recipient is a natural  
23       person other than an employee or contractor of the  
24       covered entity;

1           (2) at least one intended recipient is a person  
2           other than the covered entity; or

3           (3) a purpose of the covered entity's service is  
4           to maintain, at the direction of the sender, the con-  
5           tent of said communication for more than a transi-  
6           tory period.

7           (c) SENDER.—The sender of a communication is the  
8           person for whom the communication, and its content, is  
9           disclosed at the direction of and on behalf of.

10          (1) Where the sender is a natural person, they  
11          shall be the sender of the entire content of the com-  
12          munication, regardless of the original author of any  
13          portion of the content.

14          (2) Otherwise, a sender shall be the sender of  
15          only the content it was an original author of, or con-  
16          tent it received as an intended recipient.

17          (d) EXCEPTION FOR PUBLICLY AVAILABLE COMMU-  
18          NICATIONS.—Subsection (a) shall not apply where the con-  
19          tents of communication are made publicly accessible by the  
20          sender without restrictions on accessibility other than the  
21          general authorization to access the services used to make  
22          the information accessible.

23          (e) ENCRYPTION PROTECTION.—A covered entity  
24          shall not—

1           (1) prohibit or prevent a person from  
2       encrypting or otherwise rendering unintelligible the  
3       content of a communication using a means that pre-  
4       vents the covered entity from being able to decrypt  
5       or otherwise render intelligible said content; and

6           (2) require or cause a person to disclose or cir-  
7       cumvent the means described in paragraph (1) to  
8       the covered entity that would allow it to render the  
9       content intelligible.

10       (f) SERVICE PROVIDERS SAFE HARBOR.—A service  
11   provider shall not be held liable for a violation of this sec-  
12   tion if such service provider is acting at the direction of  
13   and on behalf of a covered entity and has a reasonable  
14   belief that the covered entity’s directions are in compliance  
15   with this section.

16   **SEC. 207. PROHIBITION ON DISCRIMINATORY PROCESSING.**

17       (a) DISCRIMINATION IN ECONOMIC OPPORTUNI-  
18   TIES.—A covered entity shall not process personal infor-  
19   mation or contents of communication for advertising, mar-  
20   keting, soliciting, offering, selling, leasing, licensing, rent-  
21   ing, or otherwise commercially contracting for employ-  
22   ment, finance, health care, credit, insurance, housing, or  
23   education opportunities in a manner that discriminates  
24   against or otherwise makes opportunities unavailable on  
25   the basis of an individual’s protected class status.

1 (b) PUBLIC ACCOMMODATIONS.—A covered entity  
2 shall not process personal information in a manner that  
3 segregates, discriminates in, or otherwise makes unavail-  
4 able the goods, services, facilities, privileges, advantages,  
5 or accommodations of any place of public accommodation  
6 on the basis of the protected class status of an individual  
7 or a group of individuals.

8 (c) REGULATIONS.—The Director shall promulgate  
9 regulations to implement this section.

10 **SEC. 208. REQUIREMENTS FOR NOTICE AND CONSENT**  
11 **PROCESSES AND PRIVACY POLICIES.**

12 (a) MINIMUM THRESHOLD.—The Director shall es-  
13 tablish minimum thresholds that covered entities must  
14 meet for the percentage of individuals who understand a  
15 notice or consent process or privacy policy required by this  
16 Act. In establishing such minimum thresholds, the Direc-  
17 tor shall—

18 (1) vary required thresholds on types and scale  
19 of reasonably foreseeable privacy harms; and

20 (2) take into account expectations of individ-  
21 uals, potential privacy harms, and individuals'  
22 awareness of privacy harms.

23 (b) CONSENT REVOCATION.—A covered entity shall  
24 make available a reasonable mechanism by which an indi-

1   vidual may revoke consent for any consent given under  
2   this Act.

3       (c) SAFE HARBOR.—

4           (1) APPROVAL PROCEDURES.—The Director  
5       shall develop procedures for analyzing and approving  
6       data submitted by a covered entity to establish that  
7       a notice and consent process or privacy policy of  
8       such covered entity meets the threshold established  
9       under subsection (a).

10          (2) PRESUMPTION.—If a covered entity submits  
11       testing data to and receives an approval from the  
12       Director under paragraph (1) establishing that a no-  
13       tice or consent process or privacy policy of such cov-  
14       ered entity meets the threshold established under  
15       subsection (a), such notice or consent process or pri-  
16       vacy policy shall be presumed to have met such  
17       threshold. Such presumption may be rebutted by  
18       clear and convincing evidence.

19          (3) PUBLIC AVAILABILITY OF APPROVED PROC-  
20       ESSES AND POLICIES AND ASSOCIATED TESTING  
21       DATA.—The Director shall make publicly available  
22       online the notice and consent processes and privacy  
23       policies and associated testing data that the Director  
24       approves under paragraph (1).

1           (4) SMALL BUSINESS ADOPTION OF NOTICE OR  
2       CONSENT PROCESS OF ANOTHER COVERED ENTI-  
3       TY.—

4           (A) IN GENERAL.—If a small business  
5       adopts a notice or consent process of another  
6       covered entity that collects, processes, main-  
7       tains, or discloses personal information in sub-  
8       stantially the same way as such small business,  
9       if the process of such other covered entity has  
10      been approved under paragraph (1), the process  
11      of such small business shall receive the pre-  
12      sumption under paragraph (2).

13          (B) ABILITY TO FREELY USE APPROVED  
14      PROCESS.—A covered entity whose notice or  
15      consent process is approved under paragraph  
16      (1) shall permit a small business to freely use  
17      such process, or a derivative thereof, as de-  
18      scribed in subparagraph (A).

19          (C) NO PUBLISHED PROCESS.—In the case  
20      of a small business for which there is no ap-  
21      proved notice or consent process published  
22      under paragraph (3) of a covered entity that  
23      collects, processes, maintains, or discloses per-  
24      sonal information in substantially the same way  
25      as such small business, any requirement under



1           this title for a notice or consent process to be  
2           objectively shown to meet the threshold estab-  
3           lished by the Director under subsection (a)  
4           shall not apply to such small business. Nothing  
5           in the preceding sentence exempts a small busi-  
6           ness from the requirement to use such notice or  
7           consent process or that such process be concise  
8           and clear.

9           (D) INAPPLICABILITY TO PRIVACY POL-  
10          ICY.—Paragraph (4) does not apply with re-  
11          spect to a privacy policy.

12          (5) MINOR CHANGES.—A covered entity may  
13          make minor changes in a notice or consent process  
14          or privacy policy approved under paragraph (1) and  
15          retain the presumption under paragraph (2) for such  
16          process or policy without retesting or resubmission  
17          of testing data to the Director.

18 **SEC. 209. PROHIBITION ON “DARK PATTERNS” IN NOTICE**  
19 **AND CONSENT PROCESSES AND PRIVACY**  
20 **POLICIES.**

21          In providing notice, obtaining consent, or maintaining  
22          a privacy policy as required by this title, a covered entity  
23          may not intentionally take any action that substantially  
24          impairs, obscures, or subverts the ability of an individual  
25          to—

1           (1) understand the contents of such notice or  
2       such privacy policy;

3           (2) understand the process for granting such  
4       consent;

5           (3) make a decision regarding whether to grant  
6       or withdraw such consent; or

7           (4) act on any such decision.

8       **SEC. 210. NOTICE AND CONSENT REQUIRED.**

9       (a) NOTICE.—A covered entity shall provide an indi-  
10   vidual with notice of the personal information such covered  
11   entity collects, processes, maintains, and discloses through  
12   a process that is concise and clear and can be objectively  
13   shown to meet the threshold established by the Director  
14   under section 208(a).

15       (b) CONSENT.—

16           (1) EXPRESS CONSENT REQUIRED.—Except as  
17       provided in paragraphs (2) and (3), a covered entity  
18       may not collect from an individual personal informa-  
19       tion that creates or increases the risk of foreseeable  
20       privacy harms, or process or maintain any such per-  
21       sonal information collected from an individual, un-  
22       less such entity obtains the express consent of such  
23       individual to the collecting, processing, or maintain-  
24       ing (or any combination thereof) of such information  
25       through a process that is concise and clear and can

1 be objectively shown to meet the threshold estab-  
2 lished by the Director under section 208(a).

3 (2) EXCEPTION FOR IMPLIED CONSENT.—Not-  
4 withstanding paragraph (1), express consent is not  
5 required for collecting, processing, or maintaining  
6 personal information if the collecting, processing, or  
7 maintaining is, on its face, obvious and necessary to  
8 provide a service at the request of the individual and  
9 the personal information is collected, processed, or  
10 maintained only for such request. Nothing in this  
11 paragraph shall be construed to exempt the covered  
12 entity from the requirement of subsection (a) to pro-  
13 vide notice to such individual with respect to such  
14 collecting, processing, or maintaining.

15 (3) EXEMPTION FOR PRIVACY-PRESERVING  
16 COMPUTING.—Notwithstanding paragraph (1), ex-  
17 cept with regard to consent for purposes of section  
18 106, express consent is not required for collecting,  
19 processing, or maintaining personal information se-  
20 cured using privacy-preserving computing. Nothing  
21 in this paragraph shall be construed to exempt the  
22 covered entity from the requirement of subsection  
23 (a) to provide notice to such individual with respect  
24 to such collecting, processing, or maintaining.

1 (c) SERVICE PROVIDERS EXCLUDED.—This section  
2 does not apply to a service provider if such service provider  
3 has a reasonable belief that a covered entity for which it  
4 processes, maintains, or discloses personal information is  
5 in compliance with this section.

6 **SEC. 211. PRIVACY POLICY.**

7 (a) POLICY REQUIRED.—A covered entity shall main-  
8 tain a privacy policy relating to the practices of such entity  
9 regarding the collecting, processing, maintaining, and dis-  
10 closing of personal information.

11 (b) CONTENTS.—The privacy policy required by sub-  
12 section (a) shall contain the following:

13 (1) A general description of the practices of the  
14 covered entity regarding the collecting, processing,  
15 maintaining, and disclosing of personal information.

16 (2) A description of how individuals may exer-  
17 cise the rights provided by title I.

18 (3) A clear and concise summary of the fol-  
19 lowing:

20 (A) The categories of personal information  
21 collected or otherwise obtained by the covered  
22 entity.

23 (B) The business or commercial purposes  
24 of the covered entity for collecting, processing,  
25 maintaining, or disclosing personal information.

1 (C) The categories and a list of third par-  
2 ties to which the covered entity discloses per-  
3 sonal information.

4 (4) A description of the personal information  
5 that the covered entity maintains that the covered  
6 entity does not collect from individuals and how the  
7 covered entity obtains such personal information.

8 (5) A list of the third parties to which the cov-  
9 ered entity has disclosed personal information.

10 (6) A list of the third parties from which the  
11 covered entity has obtained personal information at  
12 any time on or after the effective date of this Act.

13 (7) The articulated basis for the collecting,  
14 processing, disclosing, and maintaining of personal  
15 information, as required under section 201(a).

16 (c) EXEMPTION FOR PERSONAL INFORMATION FOR  
17 PARTICULAR PURPOSES.—The privacy policy required by  
18 subsection (a) is not required to contain information relat-  
19 ing to personal information that is collected, processed,  
20 maintained, or disclosed exclusively for any of the pur-  
21 poses described in paragraph (1) of section 109(a) (or a  
22 combination of such purposes), except as provided in para-  
23 graph (2) of such section.

24 (d) AVAILABILITY OF PRIVACY POLICY.—

1           (1) FORM AND MANNER.—The privacy policy  
2       required by subsection (a) shall be—

3                   (A) clear and in plain language; and

4                   (B) made publicly available in a prominent  
5       location on an ongoing basis.

6           (2) TIMING.—The privacy policy required by  
7       subsection (a) shall be made available as required by  
8       paragraph (1) before the covered entity collects per-  
9       sonal information after the effective date of this Act.

10       (e) SMALL BUSINESSES EXCLUDED.—Subsections  
11   (b)(7) and (d) do not apply to a small business.

12       (f) SERVICE PROVIDERS EXCLUDED.—This section  
13   does not apply to a service provider if such service provider  
14   has a reasonable belief that a covered entity for which it  
15   processes, maintains, or discloses personal information is  
16   in compliance with this section.

17   **SEC. 212. INFORMATION SECURITY REQUIREMENTS.**

18       (a) IN GENERAL.—A covered entity shall establish  
19   and implement reasonable information security policies,  
20   practices, and procedures for the protection of personal  
21   information collected, processed, maintained, or disclosed  
22   by such covered entity, taking into consideration—

23                   (1) the nature, scope, and complexity of the ac-  
24       tivities engaged in by such covered entity;

1           (2) the sensitivity of any personal information  
2       at issue;

3           (3) the current state of the art in administra-  
4       tive, technical, and physical safeguards for pro-  
5       tecting such information; and

6           (4) the cost of implementing such administra-  
7       tive, technical, and physical safeguards.

8       (b) SPECIFIC POLICIES, PRACTICES, AND PROCE-  
9       DURES.—The policies, practices, and procedures required  
10     by subsection (a) shall include the following:

11           (1) A written security policy with respect to col-  
12       lecting, processing, maintaining, and disclosing of  
13       personal information. Such policy shall be made pub-  
14       licly available in a prominent location on an ongoing  
15       basis, except that the publicly available version is  
16       not required to contain information that would com-  
17       promise a purpose described in section 109(a)(1).

18           (2) A process for identifying and assessing rea-  
19       sonably foreseeable security vulnerabilities in the  
20       system or systems used by such covered entity that  
21       contain personal information, which shall include  
22       regular monitoring for vulnerabilities or data  
23       breaches involving such system or systems.

24           (3) A process for taking action designed to  
25       mitigate against vulnerabilities identified in the

1 process required by paragraph (2), which may in-  
2 clude implementing any changes to security practices  
3 and the architecture, installation, or implementation  
4 of network or operating software, or for regularly  
5 testing or otherwise monitoring the effectiveness of  
6 the existing safeguards.

7 (4) A process for determining if personal infor-  
8 mation is no longer needed and disposing of personal  
9 information by shredding, permanently erasing, or  
10 otherwise modifying the medium on which such per-  
11 sonal information is maintained to make such per-  
12 sonal information permanently unreadable or indeci-  
13 pherable.

14 (5) A process for overseeing persons who have  
15 access to personal information, including through  
16 network-connected devices.

17 (6) A process for employee training and super-  
18 vision for implementation of the policies, practices,  
19 and procedures required by this section.

20 (7) A written plan or protocol for internal and  
21 public response in the event of a data breach or  
22 data-sharing abuse.

23 (c) REGULATIONS.—The Director, in consultation  
24 with the Cybersecurity and Infrastructure Security Agen-  
25 cy and the National Institute of Standards and Tech-



1 nology, shall promulgate regulations to implement this  
2 section.

3 (d) SMALL BUSINESSES ASSISTANCE.—The Director,  
4 in consultation with the Cybersecurity and Infrastructure  
5 Security Agency, the National Institute of Standards and  
6 Technology, the Small Business Administration, the Mi-  
7 nority Business Development Agency, and small busi-  
8 nesses, shall develop policy templates, toolkits, tip sheets,  
9 configuration guidelines for commonly used hardware and  
10 software, interactive tools, and other materials to assist  
11 small businesses with complying with this section.

12 **SEC. 213. NOTIFICATION OF DATA BREACH OR DATA-SHAR-**  
13 **ING ABUSE.**

14 (a) NOTIFICATION OF AGENCY.—

15 (1) IN GENERAL.—In the case of a data breach  
16 or data-sharing abuse with respect to personal infor-  
17 mation maintained by a covered entity, such covered  
18 entity shall, without undue delay and, if feasible, not  
19 later than 72 hours after becoming aware of such  
20 data breach or data-sharing abuse, notify the Direc-  
21 tor of such data breach or data-sharing abuse, un-  
22 less such data breach or data-sharing abuse is un-  
23 likely to create or increase foreseeable privacy  
24 harms.

1           (2) REASONS FOR DELAY.—If the notification  
2       required by paragraph (1) is made more than 72  
3       hours after the covered entity becomes aware of the  
4       data breach or data-sharing abuse, such notification  
5       shall be accompanied by a statement of the reasons  
6       for the delay.

7       (b) NOTIFICATION OF OTHER COVERED ENTITY.—  
8   In the case of a data breach or data-sharing abuse with  
9   respect to personal information maintained by a covered  
10   entity that such covered entity obtained from another cov-  
11   ered entity, the covered entity experiencing such data  
12   breach or data-sharing abuse shall, without undue delay  
13   and, if feasible, not later than 72 hours after becoming  
14   aware of such data breach or data-sharing abuse, notify  
15   such other covered entity of such data breach or data-  
16   sharing abuse, unless such data breach or data-sharing  
17   abuse is unlikely to create or increase foreseeable privacy  
18   harms. A covered entity receiving notice under this sub-  
19   section of a data breach or data-sharing abuse shall notify  
20   any other covered entity from which the covered entity re-  
21   ceiving notice obtained personal information involved in  
22   such data breach or data-sharing abuse, in the same man-  
23   ner as required under the preceding sentence for the cov-  
24   ered entity experiencing such data breach or data-sharing  
25   abuse.

1 (c) NOTIFICATION OF INDIVIDUALS.—

2 (1) IN GENERAL.—In the case of a data breach  
3 or data-sharing abuse with respect to personal infor-  
4 mation maintained by a covered entity (or a data  
5 breach or data-sharing abuse about which a covered  
6 entity is notified under subsection (b)), if such cov-  
7 ered entity has a relationship with an individual  
8 whose personal information was involved or poten-  
9 tially involved in such data breach or data-sharing  
10 abuse, such covered entity shall notify such indi-  
11 vidual of such data breach or data-sharing abuse not  
12 later than 14 days after becoming aware of such  
13 data breach or data-sharing abuse (or, in the case  
14 of a data breach or data-sharing abuse about which  
15 a covered entity is notified under subsection (b), not  
16 later than 14 days after being so notified), if such  
17 data breach or data-sharing abuse creates or in-  
18 creases foreseeable privacy harms.

19 (2) MEDIUM OF NOTIFICATION.—A covered en-  
20 tity shall notify an individual as required by para-  
21 graph (1) through—

22 (A) the same medium through which such  
23 individual routinely interacts with such covered  
24 entity; and

1 (B) one additional medium of notification,  
2 if such covered entity has the personal informa-  
3 tion necessary to make a notification through  
4 such an additional medium without causing ex-  
5 cessive financial burden for such covered entity.

6 (d) RULE OF CONSTRUCTION.—This section shall not  
7 apply to a covered entity if a person uses personal infor-  
8 mation obtained from a data breach or data-sharing abuse  
9 not involving such covered entity.

## 10 **TITLE III—DIGITAL PRIVACY** 11 **AGENCY**

### 12 **SEC. 301. ESTABLISHMENT; DIRECTOR AND DEPUTY DIREC-** 13 **TOR.**

14 (a) AGENCY ESTABLISHED.—There is established an  
15 independent agency in the executive branch to be known  
16 as the “Digital Privacy Agency”, which shall implement  
17 and enforce this Act.

18 (b) DIRECTOR.—

19 (1) IN GENERAL.—There is established the po-  
20 sition of the Director, who shall serve as the head  
21 of the Agency.

22 (2) APPOINTMENT.—Subject to paragraph (3),  
23 the Director shall be appointed by the President, by  
24 and with the advice and consent of the Senate.

1           (3) QUALIFICATION.—The President shall  
2           nominate the Director who, by reason of professional  
3           background and experience, is especially qualified to  
4           lead the Agency based on their knowledge and exper-  
5           tise in—

6                   (A) privacy;

7                   (B) information security;

8                   (C) technology; and

9                   (D) civil rights and civil liberties.

10          (4) TERM.—

11               (A) IN GENERAL.—The Director shall  
12               serve for a term of 6 years.

13               (B) EXPIRATION OF TERM.—An individual  
14               may serve as Director after the expiration of  
15               the term for which appointed, until a successor  
16               has been appointed and qualified.

17          (5) COMPENSATION.—

18               (A) IN GENERAL.—The Director shall be  
19               compensated at the rate prescribed for level II  
20               of the Executive Schedule under section 5313  
21               of title 5, United States Code.

22               (B) CONFORMING AMENDMENT.—Section  
23               5313 of title 5, United States Code, is amended  
24               by inserting after the item relating to the  
25               “Chief Executive Officer, United States Inter-

1           national Development Finance Corporation.”  
2           the following new item: “Director of the Digital  
3           Privacy Agency.”.

4           (c) DEPUTY DIRECTOR.—There is established the po-  
5   sition of Deputy Director, who shall—

6           (1) be appointed by the Director; and

7           (2) serve as acting Director in the absence or  
8   unavailability of the Director, notwithstanding sec-  
9   tion 3345 of title 5, United States Code.

10          (d) SERVICE RESTRICTION.—No Director or Deputy  
11   Director may hold any office, position, or employment in  
12   any covered entity during the period of service of such per-  
13   son as Director or Deputy Director.

14          (e) OFFICES.—The Director shall establish a prin-  
15   cipal office and field offices of the Agency in locations that  
16   have high levels of activity by covered entities, as deter-  
17   mined by the Director.

18   **SEC. 302. AGENCY POWERS AND AUTHORITIES.**

19          (a) POWERS OF THE AGENCY.—The Director is au-  
20   thorized to establish the general policies of the Agency  
21   with respect to all executive and administrative functions,  
22   including—

23           (1) establishing of rules for conducting the gen-  
24   eral business of the Agency, in a manner not incon-  
25   sistent with this Act;

1           (2) binding the Agency and enter into con-  
2       tracts;

3           (3) directing the establishment and continued  
4       operation of divisions or other offices within the  
5       Agency, in order to carry out the responsibilities of  
6       the Agency under this Act, and to satisfy the re-  
7       quirements of other applicable law;

8           (4) coordinating and overseeing the operation of  
9       all administrative, enforcement, and research activi-  
10      ties of the Agency;

11          (5) adopting and using a seal;

12          (6) determining the character of and the neces-  
13      sity for the obligations and expenditures of the  
14      Agency;

15          (7) appointing and supervising of personnel em-  
16      ployed by the Agency;

17          (8) distributing business among personnel ap-  
18      pointed and supervised by the Director and among  
19      administrative units of the Agency;

20          (9) using and expending of funds;

21          (10) implementing this Act through rules, or-  
22      ders, guidance, interpretations, statements of policy,  
23      investigations, and enforcement actions; and

24          (11) performing such other functions as may be  
25      authorized or required by law.

1 (b) DELEGATION OF AUTHORITY.—The Director  
2 may delegate to any duly authorized employee, representa-  
3 tive, or agent any power vested in the Director or the  
4 Agency by law, except that the Director may not delegate  
5 the power to appoint the Deputy Director under section  
6 301(c).

7 (c) AUTONOMY OF AGENCY REGARDING REC-  
8 OMMENDATIONS AND TESTIMONY.—No officer or agency  
9 of the United States shall have any authority to require  
10 the Director or any other officer of the Agency to submit  
11 legislative recommendations, or testimony or comments on  
12 legislation, to any officer or agency of the United States  
13 for approval, comments, or review prior to the submission  
14 of such recommendations, testimony, or comments to the  
15 Congress, if such recommendations, testimony, or com-  
16 ments to the Congress include a statement indicating that  
17 the views expressed therein are those of the Director or  
18 such officer, and do not necessarily reflect the views of  
19 the President.

20 (d) RULEMAKING AUTHORITY.—

21 (1) IN GENERAL.—The Director may prescribe  
22 rules and issue orders and guidance, as may be nec-  
23 essary or appropriate to enable the Agency to imple-  
24 ment, administer, and carry out the purposes and



1 objectives of this Act, and to prevent evasions there-  
2 of.

3 (2) REGULATIONS.—The Agency may issue reg-  
4 ulations after notice and comment in accordance  
5 with section 553 of title 5, United States Code, as  
6 may be necessary to implement, administer, and  
7 carry out this Act.

8 (e) CONSULTATIONS.—In implementing or enforcing  
9 this Act, the Director may consult with—

10 (1) Federal agencies that have—

11 (A) jurisdiction over Federal privacy laws;

12 and

13 (B) expertise in privacy or information se-  
14 curity;

15 (2) State attorneys general, State privacy regu-  
16 lators, and other State agencies that have expertise  
17 in privacy or information security;

18 (3) international and intergovernmental bodies  
19 that conduct activities relating to the privacy or in-  
20 formation security;

21 (4) agencies of other countries that are similar  
22 to the Agency or have expertise in privacy or infor-  
23 mation security;

24 (5) privacy and information security experts in  
25 academia, government, civil society, or industry; and

1 (6) advisory boards of the Agency established  
2 under section 308, as appropriate.

3 **SEC. 303. REPORTING AND AUDIT REQUIREMENTS.**

4 (a) REPORTS REQUIRED.—

5 (1) IN GENERAL.—Not later than 6 months  
6 after the date of the enactment of this Act, and  
7 every 6 months thereafter, the Director shall submit  
8 a report to the President and to the Committee on  
9 Energy and Commerce, the Committee on the Judi-  
10 ciary, and the Committee on Appropriations of the  
11 House of Representatives and the Committee on  
12 Commerce, Science, and Transportation, the Com-  
13 mittee on the Judiciary, and the Committee on Ap-  
14 propriations of the Senate, and shall publish such  
15 report on the website of the Agency.

16 (2) CONTENTS.—Each report required by sub-  
17 section (a) shall include—

18 (A) a discussion of the significant problems  
19 faced by individuals with respect to the privacy  
20 or security of personal information;

21 (B) a justification of the budget request of  
22 the Agency for the preceding year, unless a jus-  
23 tification for such year was included in the pre-  
24 ceding report submitted under such subsection;

1 (C) a list of the significant rules and or-  
2 ders adopted by the Agency, as well as other  
3 significant initiatives conducted by the Agency,  
4 during the preceding 6-month period and the  
5 plan of the Agency for rules, orders, or other  
6 initiatives to be undertaken during the upcom-  
7 ing 6-month period;

8 (D) an analysis of complaints about the  
9 privacy or security of personal information that  
10 the Agency has received and collected in the  
11 database described in section 307(a) during the  
12 preceding 6-month period;

13 (E) a list, with a brief statement of the  
14 issues, of the public enforcement actions to  
15 which the Agency was a party during the pre-  
16 ceding 6-month period; and

17 (F) an assessment of significant actions by  
18 State attorneys general or State privacy regu-  
19 lators relating to this Act or the rules pre-  
20 scribed under this Act during the preceding 6-  
21 month period.

22 (b) ANNUAL AUDITS.—The Director shall order an  
23 annual independent audit of the operations and budget of  
24 the Agency.

1 **SEC. 304. RELATION TO OTHER AGENCIES.**

2 (a) COORDINATION.—

3 (1) IN GENERAL.—With respect to covered enti-  
4 ties and service providers, to the extent that Federal  
5 law authorizes the Agency and another Federal  
6 agency to enforce a Federal privacy law, the other  
7 Federal agency shall coordinate with the Agency to  
8 promote consistent enforcement of this Act and the  
9 other Federal privacy law.

10 (2) REFERRAL.—Any Federal agency author-  
11 ized to enforce Federal privacy laws may recommend  
12 in writing to the Agency that the Agency initiate an  
13 enforcement proceeding, as the Agency is authorized  
14 by that Federal privacy law or by this Act.

15 (b) TRANSFERS FROM THE COMMISSION.—

16 (1) TRANSFERS OF AUTHORITY.—

17 (A) TRANSFER OF RULEMAKING AND CER-  
18 TAIN OTHER AUTHORITIES UNDER FEDERAL  
19 PRIVACY LAWS.—The Agency shall have all  
20 powers and duties under the Federal privacy  
21 laws to prescribe rules, issue guidelines, or to  
22 conduct studies or issue reports mandated by  
23 such laws, that were vested in the Commission  
24 on the effective date of this Act. The authority  
25 of the Commission under Federal privacy laws  
26 to prescribe rules, issue guidelines, or conduct

1 a study or issue a report mandated under such  
2 law shall be transferred to the Agency on the  
3 effective date of this Act.

4 (B) TRANSFER OF ENFORCEMENT AU-  
5 THORITY.—The Agency may enforce a rule pre-  
6 scribed by the Commission under—

7 (i) Federal privacy laws; or

8 (ii) the Federal Trade Commission  
9 Act (15 U.S.C. 41 et seq.) related to un-  
10 fair or deceptive acts or practices relating  
11 to privacy, information security, identity  
12 theft, data abuses, and related matters  
13 shall be transferred to the Agency.

14 (2) TRANSFER OF PRIVACY EMPLOYEES.—Any  
15 employee of the Commission employed in a division,  
16 bureau, office, or other subdivision of the Commis-  
17 sion with the primary responsibility of admin-  
18 istering, investigating, or enforcing Federal privacy  
19 laws or applications of the Federal Trade Commis-  
20 sion Act (15 U.S.C. 41 et seq.) related to unfair or  
21 deceptive acts or practices relating to privacy, infor-  
22 mation security, identity theft, data abuses, and re-  
23 lated matters shall be transferred to the Agency.  
24 Such employee shall be provided with compensation  
25 and benefits not less than the equivalent of com-

1       pensation and benefits provided to such employee on  
2       the date of enactment of this Act or compensation  
3       and benefits provided to an employee of the Agency  
4       in comparable position with comparable experience.

5       (c) PRESERVATION OF AUTHORITIES OF OTHER  
6 AGENCIES.—Except as described in this section, no provi-  
7 sion of this Act shall be construed as modifying, limiting,  
8 or otherwise affecting the operation of any provision of  
9 Federal law, or otherwise affecting the authority of any  
10 Federal agency under a Federal privacy law or any other  
11 law, including the ability of such Federal agency to pro-  
12 mulgate regulations and enforce Federal privacy laws.

13 **SEC. 305. PERSONNEL.**

14       (a) PERSONNEL.—

15           (1) APPOINTMENT GENERALLY.—The Director  
16       may fix the number of, and appoint and direct, all  
17       employees of the Agency, in accordance with the ap-  
18       plicable provisions of title 5, United States Code.  
19       The Director may appoint personnel without regard  
20       to the provisions of title 5, United States Code, gov-  
21       erning appointments in the competitive service, so  
22       long as the Director sets requirements, conducts re-  
23       cruitment, and determines appointments in a fair,  
24       transparent, and equitable manner.

1           (2) EMPLOYEES OF THE AGENCY.—The Direc-  
2       tor is authorized to employ privacy experts, tech-  
3       nologists, computer scientists, user experience de-  
4       signers and researchers, data scientists, ethicists, at-  
5       torneys, investigators, economists, civil rights ex-  
6       perts, and other employees as the Director considers  
7       necessary to conduct the business of the Agency.  
8       Unless otherwise provided expressly by law, any indi-  
9       vidual appointed under this section shall be an em-  
10      ployee, as defined in section 2105 of title 5, United  
11      States Code, and subject to the provisions of such  
12      title and other laws generally applicable to the em-  
13      ployees of an executive agency.

14          (3) EMPLOYEE COMPENSATION.—The Director  
15      may fix and adjust the pay and benefits of personnel  
16      as the Director considers desirable, competitive,  
17      transparent, and equitable, without regard to the  
18      provisions of chapter 51 and subchapter III of chap-  
19      ter 53 of title 5, United States Code, relating to  
20      classification and General Schedule pay rates, re-  
21      spectively.

22          (4) LABOR-MANAGEMENT RELATIONS.—Chap-  
23      ter 71 of title 5, United States Code, shall apply to  
24      the Agency and the employees of the Agency.

25      (b) ADDITIONAL ROLES.—

1 (1) CHIEF INFORMATION OFFICER.—

2 (A) DESIGNATION OF AN AGENCY CIO.—

3 Subchapter II of chapter 113 of subtitle III of  
4 title 40, United States Code, is amended—

5 (i) in section 11315(c) by adding  
6 “and of the Digital Privacy Agency” before  
7 the em-dash immediately preceding para-  
8 graph (1); and

9 (ii) in section 11319(a)(1) by adding  
10 “and the Digital Privacy Agency” before  
11 the period.

12 (B) RESPONSIBILITY.—The Chief Informa-  
13 tion Officer of the Digital Privacy Agency, as  
14 designated by subparagraph (A), shall ensure  
15 the Digital Privacy Agency uses technology effi-  
16 ciency to implement, administer, and enforce  
17 this Act and the rules and orders issued pursu-  
18 ant to this Act.

19 (2) INSPECTOR GENERAL.—Section 12 of the  
20 Inspector General Act of 1978 (5 U.S.C. App.) is  
21 amended—

22 (A) in paragraph (1), by inserting “the Di-  
23 rector of the Digital Privacy Agency;” after  
24 “the President of the Export-Import Bank;”;  
25 and



1 (B) in paragraph (2), by inserting “the  
2 Digital Privacy Agency,” after “the Export-Im-  
3 port Bank,”.

4 (3) OMBUD.—The Director shall appoint an  
5 ombud who shall—

6 (A) act as a liaison between the Agency  
7 and any affected person with respect to any  
8 problem that such person may have in dealing  
9 with the Agency that result from the regulatory  
10 activities of the Agency; and

11 (B) assure that safeguards exist to encour-  
12 age complainants to come forward and preserve  
13 confidentiality.

14 (c) AUTHORITY TO ACCEPT FEDERAL DETAILEES.—  
15 The Director may accept officers or employees of the  
16 United States or members of the Armed Forces on a detail  
17 from an element of the Federal Government on a nonreim-  
18 bursable basis, as jointly agreed to by the heads of the  
19 receiving and detailing elements, for a period not to exceed  
20 3 years.

21 **SEC. 306. OFFICE OF CIVIL RIGHTS.**

22 The Director shall establish an Office of Civil Rights  
23 within the Agency that shall have following responsibil-  
24 ities:

1           (1) Providing oversight and enforcement of this  
2     Act, rules and orders issued pursuant to this Act,  
3     and Federal privacy laws to ensure that collecting,  
4     processing, maintaining, and disclosing of personal  
5     information is fair, equitable, and non-discrimina-  
6     tory in treatment and effect, including through the  
7     implementation and enforcement of section 207.

8           (2) Developing, establishing, and promoting  
9     practices that affirmatively further equal oppor-  
10    tunity to and expand access to employment (includ-  
11    ing hiring, firing, promotion, demotion, and com-  
12    pensation), credit and insurance (including denial of  
13    an application or obtaining less favorable terms),  
14    housing, education, professional certification, or the  
15    provision of health care and related services.

16          (3) Coordinating the Agency's civil rights ef-  
17    forts with other Federal agencies and State regu-  
18    lators, as appropriate, to promote consistent, effi-  
19    cient, and effective enforcement of Federal civil  
20    rights laws.

21          (4) Working with civil rights advocates, privacy  
22    experts, and other experts (including members of the  
23    advisory boards established under section 308) on  
24    the promotion of compliance with the civil rights

1 provisions under this Act, rules and orders issued  
2 pursuant this Act, and Federal privacy laws.

3 (5) Liaising with communities and consumers  
4 impacted by practices regulated by this Act and the  
5 Agency, to ensure that their needs and views are ap-  
6 propriately taken into account.

7 (6) Providing annual reports to Congress on the  
8 efforts of the Agency to fulfill its civil rights man-  
9 date.

10 (7) Such additional powers and duties as the  
11 Director may determine are appropriate.

12 **SEC. 307. COMPLAINTS OF INDIVIDUALS.**

13 (a) IN GENERAL.—The Director shall establish a unit  
14 within the Agency the functions of which shall include es-  
15 tablishing a single, toll-free telephone number, a website,  
16 and a database or utilizing an existing database to facili-  
17 tate the centralized collection of, monitoring of, and re-  
18 sponse to complaints of individuals regarding the privacy  
19 or security of personal information. The Director shall co-  
20 ordinate with other Federal agencies with jurisdiction over  
21 Federal privacy laws to route complaints to such agencies,  
22 where appropriate.

23 (b) ROUTING COMPLAINTS TO STATES.—To the ex-  
24 tent practicable, State agencies (including State privacy

1 regulators) may receive appropriate complaints from the  
2 systems established under subsection (a), if—

3 (1) the State agency system has the functional  
4 capacity to receive calls or electronic reports routed  
5 by the Agency systems;

6 (2) the State agency has satisfied any condi-  
7 tions of participation in the system that the Agency  
8 may establish, including treatment of personal infor-  
9 mation and sharing of information on complaint res-  
10 olution or related compliance procedures and re-  
11 sources; and

12 (3) participation by the State agency includes  
13 measures necessary to provide for protection of per-  
14 sonal information that conform to the standards for  
15 protection of the confidentiality of personal informa-  
16 tion and for data integrity and security that apply  
17 to Federal agencies.

18 (c) DATA SHARING REQUIRED.—To facilitate inclu-  
19 sion in the reports required by section 303 of the matters  
20 regarding complaints of individuals required by subsection  
21 (a)(2)(D) of such section to be included in such reports,  
22 investigation and enforcement activities, and monitoring  
23 of the privacy and security of personal information, the  
24 Agency shall share information about complaints of indi-  
25 viduals with Federal and State agencies (including State

1 privacy regulators) that have jurisdiction over the privacy  
2 or security of personal information and State attorneys  
3 general, subject to the standards applicable to Federal  
4 agencies for the protection of the confidentiality of per-  
5 sonal information and for information security and integ-  
6 rity. Other Federal agencies that have jurisdiction over the  
7 privacy or security of personal information shall share  
8 data relating to complaints of individuals regarding the  
9 privacy or security of personal information with the Agen-  
10 cy, subject to the standards applicable to Federal agencies  
11 for the protection of confidentiality of personal informa-  
12 tion and for information security and integrity.

13 (d) PUBLISHING OF COMPLAINTS.—

14 (1) CONSENT REQUIRED.—In collecting a com-  
15 plaint from an individual, the Agency shall request  
16 consent for publishing the complaint without any in-  
17 formation identifying the individual.

18 (2) PUBLIC DATABASE.—The Agency shall  
19 make publicly available on its website a database of  
20 each complaint for which it has received consent to  
21 publish the complaint from an individual who pro-  
22 vided the complaint to the Agency.

23 (3) REDACTING INFORMATION.—When nec-  
24 essary, the Agency may redact information from a

1 published complaint to protect the privacy of the in-  
2 dividual.

3 **SEC. 308. ADVISORY BOARDS.**

4 (a) ESTABLISHMENT.—The Director shall establish  
5 the following advisory boards to advise and consult with  
6 the Agency in the exercise of its functions under this Act,  
7 and to provide information on emerging practices relating  
8 to the treatment of personal information by covered enti-  
9 ties:

10 (1) The User Advisory Board, which shall be  
11 comprised of experts in consumer protection, pri-  
12 vacy, civil rights, and ethics.

13 (2) The Research Advisory Board, which shall  
14 be comprised of individuals with academic and re-  
15 search expertise in privacy, cybersecurity, computer  
16 science, innovation, design, ethics, economics, law,  
17 and public policy.

18 (3) The Startup Advisory Board, which shall be  
19 comprised of representatives of small businesses and  
20 investors in small businesses.

21 (4) The Product Advisory Board, which shall be  
22 comprised of technologists, computer scientists, de-  
23 signers, product managers, attorneys, and other rep-  
24 resentatives of covered entities.

1 (b) APPOINTMENTS.—The Director shall appoint  
2 members to the advisory boards established under sub-  
3 section (a) without regard to party affiliation.

4 (c) MEETINGS.—Each advisory board established  
5 under subsection (a) shall meet from time to time at the  
6 call of the Director, but, at a minimum, shall meet at least  
7 twice in each calendar year.

8 (d) COMPENSATION AND TRAVEL EXPENSES.—Mem-  
9 bers of the advisory boards established under subsection  
10 (a) who are not full-time employees of the United States  
11 shall—

12 (1) be entitled to receive compensation at a rate  
13 fixed by the Director while attending meetings of the  
14 advisory board, including travel time; and

15 (2) receive travel expenses, including per diem  
16 in lieu of subsistence, in accordance with applicable  
17 provisions under subchapter I of chapter 57 of title  
18 5, United States Code.

19 **SEC. 309. AUTHORIZATION OF APPROPRIATIONS.**

20 There are authorized to be appropriated to the Direc-  
21 tor to carry out this Act \$550,000,000 for each of the  
22 fiscal years 2024, 2025, 2026, 2027, and 2028.

1           **TITLE IV—ENFORCEMENT**

2   **SEC. 401. INVESTIGATIONS AND ADMINISTRATIVE DIS-**  
3           **COVERY.**

4           (a) JOINT INVESTIGATIONS.—The Agency or, where  
5 appropriate, an Agency investigator, may conduct inves-  
6 tigations and make requests for information, as authorized  
7 under this Act, on a joint basis with another Federal agen-  
8 cy, a State attorney general, or a State privacy regulator.

9           (b) SUBPOENAS.—

10           (1) IN GENERAL.—The Agency or an Agency  
11 investigator may issue subpoenas for the attendance  
12 and testimony of witnesses and the production of  
13 relevant papers, books, documents, or other material  
14 in connection with hearings under this Act.

15           (2) FAILURE TO OBEY.—In the case of contu-  
16 macy or refusal to obey a subpoena issued pursuant  
17 to this subsection and served upon any person, the  
18 district court of the United States for any district in  
19 which such person is found, resides, or transacts  
20 business, upon application by the Agency or an  
21 Agency investigator and after notice to such person,  
22 may issue an order requiring such person to appear  
23 and give testimony or to appear and produce docu-  
24 ments or other material.



1           (3) CONTEMPT.—Any failure to obey an order  
2           of the court under paragraph (2) may be punished  
3           by the court as a contempt thereof.

4           (c) DEMANDS.—

5           (1) IN GENERAL.—Whenever the Agency has  
6           reason to believe that any person may be in posses-  
7           sion, custody, or control of any documentary mate-  
8           rial or tangible things, or may have any information,  
9           relevant to a violation, the Agency may, before the  
10          institution of any proceedings under this Act, issue  
11          in writing, and cause to be served upon such person,  
12          a civil investigative demand requiring such person  
13          to—

14                (A) produce such documentary material for  
15                inspection and copying or reproduction in the  
16                form or medium requested by the Agency;

17                (B) submit such tangible things;

18                (C) file written reports or answers to ques-  
19                tions;

20                (D) give oral testimony concerning docu-  
21                mentary material, tangible things, or other in-  
22                formation; or

23                (E) furnish any combination of such mate-  
24                rial, answers, or testimony.

1           (2) REQUIREMENTS.—Each civil investigative  
2 demand shall state the nature of the conduct consti-  
3 tuting the alleged violation which is under investiga-  
4 tion and the provision of law applicable to such vio-  
5 lation.

6           (3) PRODUCTION OF DOCUMENTS.—Each civil  
7 investigative demand for the production of documen-  
8 tary material shall—

9           (A) describe each class of documentary  
10 material to be produced under the demand with  
11 such definiteness and certainty as to permit  
12 such material to be fairly identified;

13           (B) prescribe a return date or dates which  
14 will provide a reasonable period of time within  
15 which the material so demanded may be assem-  
16 bled and made available for inspection and  
17 copying or reproduction; and

18           (C) identify the custodian to whom such  
19 material shall be made available.

20           (4) PRODUCTION OF THINGS.—Each civil inves-  
21 tigative demand for the submission of tangible  
22 things shall—

23           (A) describe each class of tangible things  
24 to be submitted under the demand with such

1           definiteness and certainty as to permit such  
2           things to be fairly identified;

3           (B) prescribe a return date or dates which  
4           will provide a reasonable period of time within  
5           which the things so demanded may be assem-  
6           bled and submitted; and

7           (C) identify the custodian to whom such  
8           things shall be submitted.

9           (5) DEMAND FOR WRITTEN REPORTS OR AN-  
10          SWERS.—Each civil investigative demand for written  
11          reports or answers to questions shall—

12           (A) propound with definiteness and cer-  
13           tainty the reports to be produced or the ques-  
14           tions to be answered;

15           (B) prescribe a date or dates at which time  
16           written reports or answers to questions shall be  
17           submitted; and

18           (C) identify the custodian to whom such  
19           reports or answers shall be submitted.

20          (6) ORAL TESTIMONY.—Each civil investigative  
21          demand for the giving of oral testimony shall—

22           (A) prescribe a date, time, and place at  
23           which oral testimony shall be commenced; and

24           (B) identify an Agency investigator who  
25           shall conduct the investigation and the custo-

1           dian to whom the transcript of such investiga-  
2           tion shall be submitted.

3           (7) SERVICE.—Any civil investigative demand  
4           issued, and any enforcement petition filed, under  
5           this section may be served—

6                   (A) by any Agency investigator at any  
7                   place within the territorial jurisdiction of any  
8                   court of the United States; and

9                   (B) upon any person who is not found  
10                  within the territorial jurisdiction of any court of  
11                  the United States—

12                          (i) in such manner as the Federal  
13                          Rules of Civil Procedure prescribe for serv-  
14                          ice in a foreign nation; and

15                          (ii) to the extent that the courts of  
16                          the United States have authority to assert  
17                          jurisdiction over such person, consistent  
18                          with due process, the United States Dis-  
19                          trict Court for the District of Columbia  
20                          shall have the same jurisdiction to take  
21                          any action respecting compliance with this  
22                          section by such person that such district  
23                          court would have if such person were per-  
24                          sonally within the jurisdiction of such dis-  
25                          trict court.

1           (8) METHOD OF SERVICE.—Service of any civil  
2       investigative demand or any enforcement petition  
3       filed under this section may be made upon a person  
4       by—

5           (A) delivering a duly executed copy of such  
6       demand or petition to the individual or to any  
7       partner, executive officer, managing agent, or  
8       general agent of such person, or to any agent  
9       of such person authorized by appointment or by  
10      law to receive service of process on behalf of  
11      such person;

12          (B) delivering a duly executed copy of such  
13      demand or petition to the principal office or  
14      place of business of the person to be served; or

15          (C) depositing a duly executed copy in the  
16      United States mails, by registered or certified  
17      mail, return receipt requested, duly addressed  
18      to such person at the principal office or place  
19      of business of such person.

20      (9) PROOF OF SERVICE.—

21          (A) IN GENERAL.—A verified return by the  
22      individual serving any civil investigative demand  
23      or any enforcement petition filed under this sec-  
24      tion setting forth the manner of such service  
25      shall be proof of such service.

1 (B) RETURN RECEIPTS.—In the case of  
2 service by registered or certified mail, such re-  
3 turn shall be accompanied by the return post  
4 office receipt of delivery of such demand or en-  
5 forcement petition.

6 (10) PRODUCTION OF DOCUMENTARY MATE-  
7 RIAL.—The production of documentary material in  
8 response to a civil investigative demand shall be  
9 made under a sworn certificate, in such form as the  
10 demand designates, by the person, if a natural per-  
11 son, to whom the demand is directed or, if not a  
12 natural person, by any person having knowledge of  
13 the facts and circumstances relating to such produc-  
14 tion, to the effect that all of the documentary mate-  
15 rial required by the demand and in the possession,  
16 custody, or control of the person to whom the de-  
17 mand is directed has been produced and made avail-  
18 able to the custodian.

19 (11) SUBMISSION OF TANGIBLE THINGS.—The  
20 submission of tangible things in response to a civil  
21 investigative demand shall be made under a sworn  
22 certificate, in such form as the demand designates,  
23 by the person to whom the demand is directed or,  
24 if not a natural person, by any person having knowl-  
25 edge of the facts and circumstances relating to such

1 production, to the effect that all of the tangible  
2 things required by the demand and in the posses-  
3 sion, custody, or control of the person to whom the  
4 demand is directed have been submitted to the cus-  
5 todian.

6 (12) SEPARATE ANSWERS.—Each reporting re-  
7 quirement or question in a civil investigative demand  
8 shall be answered separately and fully in writing  
9 under oath, unless it is objected to, in which event  
10 the reasons for the objection shall be stated in lieu  
11 of an answer, and it shall be submitted under a  
12 sworn certificate, in such form as the demand des-  
13 ignates, by the person, if a natural person, to whom  
14 the demand is directed or, if not a natural person,  
15 by any person responsible for answering each report-  
16 ing requirement or question, to the effect that all in-  
17 formation required by the demand and in the posses-  
18 sion, custody, control, or knowledge of the person to  
19 whom the demand is directed has been submitted.

20 (13) TESTIMONY.—

21 (A) IN GENERAL.—

22 (i) OATH AND RECORDATION.—The  
23 examination of any person pursuant to a  
24 demand for oral testimony served under  
25 this subsection shall be taken before an of-

1           ficer authorized to administer oaths and  
2           affirmations by the laws of the United  
3           States or of the place at which the exam-  
4           ination is held. The officer before whom  
5           oral testimony is to be taken shall put the  
6           witness on oath or affirmation and shall  
7           personally, or by any individual acting  
8           under the direction of and in the presence  
9           of the officer, record the testimony of the  
10          witness.

11                 (ii) TRANSCRIPTION.—The testimony  
12           shall be taken stenographically and tran-  
13           scribed.

14                 (B) PARTIES PRESENT.—Any Agency in-  
15           vestigator before whom oral testimony is to be  
16           taken shall exclude from the place where the  
17           testimony is to be taken all other persons, ex-  
18           cept the person giving the testimony, the attor-  
19           ney for that person, the officer before whom the  
20           testimony is to be taken, an investigator or rep-  
21           resentative of an agency with which the Agency  
22           is engaged in a joint investigation, and any ste-  
23           nographer taking such testimony.

24                 (C) LOCATION.—The oral testimony of any  
25           person taken pursuant to a civil investigative



1 demand shall be taken in the judicial district of  
2 the United States in which such person resides,  
3 is found, or transacts business, or in such other  
4 place as may be agreed upon by the Agency in-  
5 vestigator before whom the oral testimony of  
6 such person is to be taken and such person.

7 (D) ATTORNEY REPRESENTATION.—

8 (i) IN GENERAL.—Any person com-  
9 pelled to appear under a civil investigative  
10 demand for oral testimony pursuant to this  
11 subsection may be accompanied, rep-  
12 resented, and advised by an attorney.

13 (ii) AUTHORITY.—The attorney may  
14 advise a person described in clause (i), in  
15 confidence, either upon the request of such  
16 person or upon the initiative of the attor-  
17 ney, with respect to any question asked of  
18 such person.

19 (iii) OBJECTIONS.—A person de-  
20 scribed in clause (i), or the attorney for  
21 that person, may object on the record to  
22 any question, in whole or in part, and such  
23 person shall briefly state for the record the  
24 reason for the objection. An objection may  
25 properly be made, received, and entered

1           upon the record when it is claimed that  
2           such person is entitled to refuse to answer  
3           the question on grounds of any constitu-  
4           tional or other legal right or privilege, in-  
5           cluding the privilege against self-incrimina-  
6           tion, but such person shall not otherwise  
7           object to or refuse to answer any question,  
8           and such person or attorney shall not oth-  
9           erwise interrupt the oral examination.

10                   (iv) REFUSAL TO ANSWER.—If a per-  
11           son described in clause (i) refuses to an-  
12           swer any question—

13                           (I) the Agency may petition the  
14           district court of the United States  
15           pursuant to this section for an order  
16           compelling such person to answer  
17           such question; and

18                           (II) if the refusal is on grounds  
19           of the privilege against self-incrimina-  
20           tion, the testimony of such person  
21           may be compelled in accordance with  
22           the provisions of section 6004 of title  
23           18, United States Code.

24                   (E) TRANSCRIPTS.—For purposes of this  
25           subsection—

1 (i) after the testimony of any witness  
2 is fully transcribed, the Agency investi-  
3 gator shall afford the witness (who may be  
4 accompanied by an attorney) a reasonable  
5 opportunity to examine the transcript;

6 (ii) the transcript shall be read to or  
7 by the witness, unless such examination  
8 and reading are waived by the witness;

9 (iii) any changes in form or substance  
10 which the witness desires to make shall be  
11 entered and identified upon the transcript  
12 by the Agency investigator, with a state-  
13 ment of the reasons given by the witness  
14 for making such changes;

15 (iv) the transcript shall be signed by  
16 the witness, unless the witness in writing  
17 waives the signing, is ill, cannot be found,  
18 or refuses to sign; and

19 (v) if the transcript is not signed by  
20 the witness during the 30-day period fol-  
21 lowing the date on which the witness is  
22 first afforded a reasonable opportunity to  
23 examine the transcript, the Agency investi-  
24 gator shall sign the transcript and state on  
25 the record the fact of the waiver, illness,

1           absence of the witness, or the refusal to  
2           sign, together with any reasons given for  
3           the failure to sign.

4           (F) CERTIFICATION BY INVESTIGATOR.—

5           The Agency investigator shall certify on the  
6           transcript that the witness was duly sworn by  
7           such Agency investigator and that the tran-  
8           script is a true record of the testimony given by  
9           the witness, and the Agency investigator shall  
10          promptly deliver the transcript or send it by  
11          registered or certified mail to the custodian.

12          (G) COPY OF TRANSCRIPT.—The Agency  
13          investigator shall furnish a copy of the tran-  
14          script (upon payment of reasonable charges for  
15          the transcript) to the witness only, except that  
16          the Agency may for good cause limit such wit-  
17          ness to inspection of the official transcript of  
18          the testimony of such witness.

19          (H) WITNESS FEES.—Any witness appear-  
20          ing for the taking of oral testimony pursuant to  
21          a civil investigative demand shall be entitled to  
22          the same fees and mileage which are paid to  
23          witnesses in the district courts of the United  
24          States.

1 (d) CONFIDENTIAL TREATMENT OF DEMAND MATE-  
2 RIAL.—

3 (1) IN GENERAL.—Documentary materials and  
4 tangible things received as a result of a civil inves-  
5 tigative demand shall be subject to requirements and  
6 procedures regarding confidentiality, in accordance  
7 with rules established by the Agency.

8 (2) DISCLOSURE TO CONGRESS.—No rule es-  
9 tablished by the Agency regarding the confidentiality  
10 of materials submitted to, or otherwise obtained by,  
11 the Agency shall be intended to prevent disclosure to  
12 either House of Congress or to an appropriate com-  
13 mittee of the Congress, except that the Agency is  
14 permitted to adopt rules allowing prior notice to any  
15 party that owns or otherwise provided the material  
16 to the Agency and had designated such material as  
17 confidential.

18 (e) PETITION FOR ENFORCEMENT.—

19 (1) IN GENERAL.—Whenever any person fails  
20 to comply with any civil investigative demand duly  
21 served upon such person under this section, or when-  
22 ever satisfactory copying or reproduction of material  
23 requested pursuant to the demand cannot be accom-  
24 plished and such person refuses to surrender such  
25 material, the Agency, through such officers or attor-

1        neys as it may designate, may file, in the district  
2        court of the United States for any judicial district  
3        in which such person resides, is found, or transacts  
4        business, and serve upon such person, a petition for  
5        an order of such court for the enforcement of this  
6        section.

7            (2) SERVICE OF PROCESS.—All process of any  
8        court to which application may be made as provided  
9        in this subsection may be served in any judicial dis-  
10       trict.

11       (f) PETITION FOR ORDER MODIFYING OR SETTING  
12       ASIDE DEMAND.—

13            (1) IN GENERAL.—Not later than 20 days after  
14       the service of any civil investigative demand upon  
15       any person under subsection (c), or at any time be-  
16       fore the return date specified in the demand, which-  
17       ever period is shorter, or within such period exceed-  
18       ing 20 days after service or in excess of such return  
19       date as may be prescribed in writing, subsequent to  
20       service, by any Agency investigator named in the de-  
21       mand, such person may file with the Agency a peti-  
22       tion for an order by the Agency modifying or setting  
23       aside the demand.

24            (2) COMPLIANCE DURING PENDENCY.—The  
25       time permitted for compliance with the demand in

1 whole or in part, as determined proper and ordered  
2 by the Agency, shall not run during the pendency of  
3 a petition under paragraph (1) at the Agency, except  
4 that such person shall comply with any portions of  
5 the demand not sought to be modified or set aside.

6 (3) SPECIFIC GROUNDS.—A petition under  
7 paragraph (1) shall specify each ground upon which  
8 the petitioner relies in seeking relief, and may be  
9 based upon any failure of the demand to comply  
10 with the provisions of this section, or upon any con-  
11 stitutional or other legal right or privilege of such  
12 person.

13 (g) CUSTODIAL CONTROL.—At any time during  
14 which any custodian is in custody or control of any docu-  
15 mentary material, tangible things, reports, answers to  
16 questions, or transcripts of oral testimony given by any  
17 person in compliance with any civil investigative demand,  
18 such person may file, in the district court of the United  
19 States for the judicial district within which the office of  
20 such custodian is situated, and serve upon such custodian,  
21 a petition for an order of such court requiring the per-  
22 formance by such custodian of any duty imposed upon  
23 such custodian by this section or rule promulgated by the  
24 Agency.

25 (h) JURISDICTION OF COURT.—

1           (1) IN GENERAL.—Whenever any petition is  
2       filed in any district court of the United States under  
3       this section, such court shall have jurisdiction to  
4       hear and determine the matter so presented, and to  
5       enter such order or orders as may be required to  
6       carry out the provisions of this section.

7           (2) APPEAL.—Any final order entered as de-  
8       scribed in paragraph (1) shall be subject to appeal  
9       pursuant to section 1291 of title 28, United States  
10      Code.

11 **SEC. 402. HEARINGS AND ADJUDICATION PROCEEDINGS.**

12       (a) IN GENERAL.—The Agency is authorized to con-  
13      duct hearings and adjudication proceedings with respect  
14      to any person in the manner prescribed by chapter 5 of  
15      title 5, United States Code, in order to ensure or enforce  
16      compliance with this Act and the rules prescribed under  
17      this Act.

18       (b) SPECIAL RULES FOR CEASE-AND-DESIST PRO-  
19      CEEDINGS.—

20           (1) ORDERS AUTHORIZED.—

21           (A) IN GENERAL.—If, in the opinion of the  
22       Agency, a person is engaging or has engaged in  
23       an act or omission that violates any provision of  
24       this Act or a rule or order prescribed under this



1 Act, the Agency may issue and serve upon the  
2 person a notice of charges in respect thereof.

3 (B) CONTENT OF NOTICE.—The notice  
4 under subparagraph (A) shall contain a state-  
5 ment of the facts constituting the alleged viola-  
6 tion, and shall fix a time and place at which a  
7 hearing will be held to determine whether an  
8 order to cease and desist should issue against  
9 the person, such hearing to be held not earlier  
10 than 30 days nor later than 60 days after the  
11 date of service of such notice, unless an earlier  
12 or a later date is set by the Agency, at the re-  
13 quest of any person so served.

14 (C) CONSENT.—Unless a person served  
15 under subparagraph (B) appears at the hearing  
16 personally or by a duly authorized representa-  
17 tive, the person shall be deemed to have con-  
18 sented to the issuance of the cease-and-desist  
19 order.

20 (D) PROCEDURE.—In the event of consent  
21 under subparagraph (C), or if, upon the record  
22 made at any such hearing, the Agency finds  
23 that any violation specified in the notice of  
24 charges has been established, the Agency may  
25 issue and serve upon the person an order to

1           cease and desist from the violation. Such order  
2           may, by provisions which may be mandatory or  
3           otherwise, require the person to cease and de-  
4           sist from the subject act or omission, and to  
5           take affirmative action to correct the conditions  
6           resulting from any such violation.

7           (2) EFFECTIVENESS OF ORDER.—A cease-and-  
8           desist order shall become effective at the expiration  
9           of 30 days after the date of service of the order  
10          under paragraph (1)(D) (except in the case of a  
11          cease-and-desist order issued upon consent, which  
12          shall become effective at the time specified therein),  
13          and shall remain effective and enforceable as pro-  
14          vided therein, except to such extent as the order is  
15          stayed, modified, terminated, or set aside by action  
16          of the Agency or a reviewing court.

17          (3) DECISION AND APPEAL.—Any hearing pro-  
18          vided for in this subsection shall be held in the Fed-  
19          eral judicial district or in the territory in which the  
20          residence or principal office or place of business of  
21          the person is located unless the person consents to  
22          another place, and shall be conducted in accordance  
23          with the provisions of chapter 5 of title 5, United  
24          States Code. After such hearing, and not later than  
25          90 days after the Agency has notified each party to

1 the proceeding that the case has been submitted to  
2 the Agency for final decision, the Agency shall  
3 render its decision (which shall include findings of  
4 fact upon which its decision is predicated) and shall  
5 issue and serve upon each such party an order or or-  
6 ders consistent with the provisions of this section.  
7 Judicial review of any such order shall be exclusively  
8 as provided in this subsection. Unless a petition for  
9 review is timely filed in a court of appeals of the  
10 United States, as provided in paragraph (4), and  
11 thereafter until the record in the proceeding has  
12 been filed as provided in paragraph (4), the Agency  
13 may at any time, upon such notice and in such man-  
14 ner as the Agency shall determine proper, modify,  
15 terminate, or set aside any such order. Upon filing  
16 of the record as provided, the Agency may modify,  
17 terminate, or set aside any such order with permis-  
18 sion of the court.

19 (4) APPEAL TO COURT OF APPEALS.—Any  
20 party to any proceeding under this subsection may  
21 obtain a review of any order served pursuant to this  
22 subsection (other than an order issued with the con-  
23 sent of the party) by filing in the court of appeals  
24 of the United States for the circuit in which the resi-  
25 dence or principal office or place of business of the

1 party is located, or in the United States Court of  
2 Appeals for the District of Columbia Circuit, within  
3 30 days after the date of service of such order, a  
4 written petition praying that the order of the Agency  
5 be modified, terminated, or set aside. A copy of such  
6 petition shall be forthwith transmitted by the clerk  
7 of the court to the Agency, and thereupon the Agen-  
8 cy shall file in the court the record in the pro-  
9 ceeding, as provided in section 2112 of title 28,  
10 United States Code. Upon the filing of such petition,  
11 such court shall have jurisdiction, which upon the  
12 filing of the record shall, except as provided in the  
13 last sentence of paragraph (3), be exclusive, to af-  
14 firm, modify, terminate, or set aside, in whole or in  
15 part, the order of the Agency. Review of such pro-  
16 ceedings shall be had as provided in chapter 7 of  
17 title 5, United States Code. The judgment and de-  
18 cree of the court shall be final, except that the same  
19 shall be subject to review by the Supreme Court of  
20 the United States, upon certiorari, as provided in  
21 section 1254 of title 28, United States Code.

22 (5) NO STAY.—The commencement of pro-  
23 ceedings for judicial review under paragraph (4)  
24 shall not, unless specifically ordered by the court,  
25 operate as a stay of any order issued by the Agency.

1 (c) SPECIAL RULES FOR TEMPORARY CEASE-AND-  
2 DESIST PROCEEDINGS.—

3 (1) IN GENERAL.—Whenever the Agency deter-  
4 mines that the violation specified in the notice of  
5 charges served upon a person pursuant to subsection  
6 (b), or the continuation thereof, is likely to cause the  
7 person to be insolvent or otherwise prejudice the in-  
8 terests of individuals before the completion of the  
9 proceedings conducted pursuant to subsection (b),  
10 the Agency may issue a temporary order requiring  
11 the person to cease and desist from any such viola-  
12 tion and to take affirmative action to prevent or  
13 remedy such insolvency or other condition pending  
14 completion of such proceedings. Such order may in-  
15 clude any requirement authorized under this title.  
16 Such order shall become effective upon service upon  
17 the person and, unless set aside, limited, or sus-  
18 pended by a court in proceedings authorized by  
19 paragraph (2), shall remain effective and enforceable  
20 pending the completion of the administrative pro-  
21 ceedings pursuant to such notice and until such time  
22 as the Agency shall dismiss the charges specified in  
23 such notice, or if a cease-and-desist order is issued  
24 against the person, until the effective date of such  
25 order.

1           (2) APPEAL.—Not later than 10 days after a  
2       person has been served with a temporary cease-and-  
3       desist order, the person may apply to the United  
4       States district court for the judicial district in which  
5       the residence or principal office or place of business  
6       of the person is located, or the United States Dis-  
7       trict Court for the District of Columbia, for an in-  
8       junction setting aside, limiting, or suspending the  
9       enforcement, operation, or effectiveness of such  
10      order pending the completion of the administrative  
11      proceedings pursuant to the notice of charges served  
12      upon the person under subsection (b), and such  
13      court shall have jurisdiction to issue such injunction.

14      (d) SPECIAL RULES FOR ENFORCEMENT OF OR-  
15      DERS.—

16           (1) IN GENERAL.—The Agency may in its dis-  
17      cretion apply to the United States district court  
18      within the jurisdiction of which the residence or  
19      principal office or place of business of a person is lo-  
20      cated, for the enforcement of any effective and out-  
21      standing order issued under this section against  
22      such person, and such court shall have jurisdiction  
23      and power to order and require compliance with  
24      such order.

1           (2) EXCEPTION.—Except as otherwise provided  
2           in this section, no court shall have jurisdiction to af-  
3           fect by injunction or otherwise the issuance or en-  
4           forcement of any order or to review, modify, sus-  
5           pend, terminate, or set aside any such order.

6           (e) RULES.—The Agency shall prescribe rules estab-  
7           lishing such procedures as may be necessary to carry out  
8           this section.

9   **SEC. 403. LITIGATION AUTHORITY.**

10          (a) IN GENERAL.—If a person violates any provision  
11          of this Act or a rule or order prescribed under this Act,  
12          the Agency may commence a civil action against such per-  
13          son to impose a civil penalty or to seek all appropriate  
14          legal and equitable relief, including a permanent or tem-  
15          porary injunction as permitted by law.

16          (b) REPRESENTATION.—Except as provided in sub-  
17          section (e), the Agency may act in its own name and  
18          through its own attorneys enforcing any provision of this  
19          Act or rules or orders issued pursuant to this Act or in  
20          any action, suit, or other court proceeding to which the  
21          Agency is a party.

22          (c) COMPROMISE OF ACTIONS.—The Agency may  
23          compromise or settle any action, suit, or other court pro-  
24          ceeding to which the Agency is a party if such compromise  
25          is approved by the court.

1 (d) NOTICE TO THE ATTORNEY GENERAL OF THE  
2 UNITED STATES.—

3 (1) IN GENERAL.—When commencing a civil  
4 action under this Act or regulations or rules or or-  
5 ders issued pursuant to this Act, the Agency shall  
6 notify the Attorney General.

7 (2) NOTICE AND COORDINATION.—

8 (A) NOTICE OF OTHER ACTIONS.—In addi-  
9 tion to any notice required under paragraph  
10 (1), the Agency shall notify the Attorney Gen-  
11 eral concerning any action, suit, or other court  
12 proceeding to which the Agency is a party.

13 (B) COORDINATION.—In order to avoid  
14 conflicts and promote consistency regarding liti-  
15 gation of matters under Federal law, the Attor-  
16 ney General and the Agency shall consult re-  
17 garding the coordination of investigations and  
18 proceedings, including by negotiating an agree-  
19 ment for coordination not later than 180 days  
20 after the effective date of this Act. The agree-  
21 ment under this subparagraph shall include  
22 provisions to ensure that parallel investigations  
23 and proceedings involving this Act and the rules  
24 prescribed under this Act are conducted in a  
25 manner that avoids conflicts and does not im-



1           pede the ability of the Attorney General to  
2           prosecute violations of Federal criminal laws.

3           (C) RULE OF CONSTRUCTION.—Nothing in  
4           this paragraph shall be construed to limit the  
5           authority of the Agency under this Act, includ-  
6           ing the authority to interpret this Act.

7           (e) APPEARANCE BEFORE THE SUPREME COURT.—  
8           The Agency may represent itself in its own name before  
9           the Supreme Court of the United States, if the Agency  
10          makes a written request to the Attorney General within  
11          the 10-day period which begins on the date of entry of  
12          the judgment which would permit any party to file a peti-  
13          tion for writ of certiorari, and the Attorney General con-  
14          curs with such request or fails to take action within 60  
15          days of the request of the Agency.

16          (f) FORUM.—Any civil action brought under this Act  
17          or regulations or rules or orders issued pursuant to this  
18          Act may be brought in an appropriate district court of  
19          the United States or an appropriate State court.

20          (g) TIME FOR BRINGING ACTION.—Except as other-  
21          wise permitted by law or equity, no action may be brought  
22          under this Act more than 3 years after the date of dis-  
23          covery of the violation to which the action relates.

1   **SEC. 404. ENFORCEMENT BY STATES.**

2           (a) CIVIL ACTION.—In any case in which a State at-  
3   torney general or a State privacy regulator has reason to  
4   believe that an interest of the residents of a State has been  
5   or is adversely affected by any person who violates any  
6   provision of this Act or a rule or order prescribed under  
7   this Act, the State attorney general or State privacy regu-  
8   lator, as *parens patriae*, may bring a civil action on behalf  
9   of the residents of the State in an appropriate State court  
10   or an appropriate district court of the United States to—

11           (1) enjoin further violation of such provision by  
12   the defendant;

13           (2) compel compliance with such provision; or

14           (3) obtain relief under section 406.

15           (b) RIGHTS OF AGENCY.—Before initiating a civil ac-  
16   tion under subsection (a), the State attorney general or  
17   State privacy regulator, as the case may be, shall notify  
18   the Agency in writing of such civil action. Upon receiving  
19   notice with respect to a civil action, the Agency may—

20           (1) intervene in such action; and

21           (2) upon intervening—

22                   (A) be heard on all matters arising in such  
23   civil action; and

24                   (B) file petitions for appeal of a decision in  
25   such action.

1 (c) PREEMPTIVE ACTION BY AGENCY.—If the Agen-  
2 cy institutes a civil action for violation of any provision  
3 of this Act or a rule or order prescribed under this Act,  
4 no State attorney general or State privacy regulator may  
5 bring a civil action against any defendant named in the  
6 complaint of the Agency for a violation of such provision  
7 that is alleged in such complaint.

8 **SEC. 405. PRIVATE RIGHTS OF ACTION.**

9 (a) INJUNCTIVE RELIEF.—A person who is aggrieved  
10 by a violation of this Act may bring a civil action for de-  
11 claratory or injunctive relief in any court of competent ju-  
12 risdiction in any State or in an appropriate district court.

13 (b) CIVIL ACTION FOR DAMAGES.—Except for claims  
14 under rule 23 of the Federal Rules of Civil Procedure or  
15 a similar judicial procedure authorizing an action to be  
16 brought by 1 or more representatives, a person who is ag-  
17 grieved by a violation of this Act may bring a civil action  
18 for damages in any court of competent jurisdiction in any  
19 State or in an appropriate district court.

20 (c) NONPROFIT COLLECTIVE REPRESENTATION.—  
21 An individual shall have the right to appoint a nonprofit  
22 organization (as described in section 501(c)(3) of the In-  
23 ternal Revenue Code of 1986 and exempt from taxation  
24 under section 501(a) of such Code) which has been prop-  
25 erly constituted in accordance with the law, has statutory

1 objectives which are in the public interest, and is active  
2 in the field of the protection of individual rights and free-  
3 doms with regard to the protection of privacy and informa-  
4 tion security to lodge the complaint on behalf of such indi-  
5 vidual to exercise the rights referred to in this Act on be-  
6 half of such individual.

7 (1) A nonprofit may represent a class of ag-  
8 grieved individuals.

9 (2) A prevailing nonprofit shall receive reason-  
10 able compensation for expenses, including attorneys'  
11 fees.

12 (3) Individuals shall receive an equally divided  
13 share of the total damages.

14 (d) STATE APPOINTMENT.—A State may provide  
15 that any body, organization, or association referred to in  
16 subsection (c), independent of an individual's appoint-  
17 ment, has the right to lodge, in that State, a complaint  
18 with the Agency and to exercise the rights referred to in  
19 this Act if it considers that the rights of an individual  
20 under this Act have been infringed.

21 **SEC. 406. RELIEF AVAILABLE.**

22 (a) CIVIL ACTIONS AND ADJUDICATION PRO-  
23 CEEDINGS.—

24 (1) JURISDICTION.—In any civil action or any  
25 adjudication proceeding brought by the Agency, a

1 State attorney general, or State privacy regulator  
2 under any provision of this Act or a rule or order  
3 prescribed under this Act, the court or the Agency  
4 (as the case may be) shall have jurisdiction to grant  
5 any appropriate legal or equitable relief with respect  
6 to a violation of such provision.

7 (2) RELIEF.—Relief under this section may in-  
8 clude—

- 9 (A) rescission or reformation of contracts;
- 10 (B) refund of moneys;
- 11 (C) restitution;
- 12 (D) disgorgement or compensation for un-  
13 just enrichment;
- 14 (E) payment of damages or other mone-  
15 tary relief;
- 16 (F) public notification regarding the viola-  
17 tion, including the costs of notification;
- 18 (G) limits on the activities or functions of  
19 the person; and
- 20 (H) civil money penalties, as provided in  
21 subsection (c).

22 (3) NO EXEMPLARY OR PUNITIVE DAMAGES.—  
23 Nothing in this subsection shall be construed as au-  
24 thorizing the imposition of exemplary or punitive  
25 damages.

1 (b) RECOVERY OF COSTS.—In any civil action  
2 brought by the Agency, State attorney general, or State  
3 privacy regulator under any provision of this Act or a rule  
4 or order prescribed under this Act, the Agency, State at-  
5 torney general, or State privacy regulator may recover its  
6 costs in connection with prosecuting such action if the  
7 Agency or State attorney general is the prevailing party  
8 in the action.

9 (c) CIVIL MONEY PENALTY IN COURT AND ADMINIS-  
10 TRATIVE ACTIONS.—

11 (1) IN GENERAL.—Any person who violates,  
12 through any act or omission, any provision of this  
13 Act or a rule or order issued pursuant to this Act  
14 shall forfeit and pay a civil penalty under this sub-  
15 section.

16 (2) PENALTY AMOUNT.—

17 (A) IN GENERAL.—The amount of a civil  
18 penalty under this subsection may not exceed,  
19 for each violation, the product of—

20 (i) the maximum civil penalty for  
21 which a person, partnership, or corporation  
22 may be liable under section 5(m)(1)(A) of  
23 the Federal Trade Commission Act (15  
24 U.S.C. 45(m)(1)(A)) for a violation of a  
25 rule under such Act respecting unfair or

1           deceptive acts or practices, as adjusted  
2           under the Federal Civil Penalties Inflation  
3           Adjustment Act of 1990 (28 U.S.C. 2461  
4           note); and

5           (ii) the number of individuals whose  
6           personal information is affected by the vio-  
7           lation.

8           (B) CONTINUING VIOLATIONS.—In the  
9           case of a violation through continuing failure to  
10          comply with a provision of this Act or a rule or  
11          order prescribed under this Act, each day of  
12          continuance of such failure shall be treated as  
13          a separate violation for purposes of subpara-  
14          graph (A).

15          (3) MITIGATING FACTORS.—In determining the  
16          amount of any penalty assessed under paragraph  
17          (2), the court or the Agency shall take into account  
18          the appropriateness of the penalty with respect to—

19                (A) the size of financial resources and good  
20                faith of the person charged;

21                (B) the gravity of the violation;

22                (C) the severity of the privacy harms (in-  
23                cluding both actual and potential harms) to in-  
24                dividuals;

1 (D) any disparate impact of the privacy  
2 harms (including both actual and potential  
3 harms) on protected classes;

4 (E) the history of previous violations; and

5 (F) such other matters as justice may re-  
6 quire.

7 (4) AUTHORITY TO MODIFY OR REMIT PEN-  
8 ALTY.—The Agency, State attorney general, or State  
9 privacy regulator may compromise, modify, or remit  
10 any penalty which may be assessed or has already  
11 been assessed under paragraph (2). The amount of  
12 such penalty, when finally determined, shall be ex-  
13 clusive of any sums owed by the person to the  
14 United States in connection with the costs of the  
15 proceeding, and may be deducted from any sums  
16 owing by the United States to the person charged.

17 (5) NOTICE AND HEARING.—No civil penalty  
18 may be assessed under this subsection with respect  
19 to a violation of any provision of this Act or a rule  
20 or order issued pursuant to this Act, unless—

21 (A) the Agency, State attorney general, or  
22 State privacy regulator gives notice and an op-  
23 portunity for a hearing to the person accused of  
24 the violation; or



1 (B) the appropriate court has ordered such  
2 assessment and entered judgment in favor of  
3 the Agency, State attorney general, or State  
4 privacy regulator.

5 **SEC. 407. REFERRAL FOR CRIMINAL PROCEEDINGS.**

6 If the Agency obtains evidence that any person, do-  
7 mestic or foreign, has engaged in conduct that may con-  
8 stitute a violation of Federal criminal law, the Agency  
9 shall transmit such evidence to the Attorney General of  
10 the United States, who may institute criminal proceedings  
11 under appropriate law. Nothing in this section affects any  
12 other authority of the Agency to disclose information.

13 **SEC. 408. WHISTLEBLOWER ENFORCEMENT.**

14 (a) IN GENERAL.—Any person who becomes aware,  
15 based on nonpublic information, that a covered entity has  
16 violated this Act may file a civil action for civil penalties,  
17 if prior to filing such action, the person files with the Di-  
18 rector a written request for the Director to commence the  
19 action. The request shall include a clear and concise state-  
20 ment of the grounds for believing a cause of action exists.  
21 The person shall make the nonpublic information available  
22 to the Director upon request:

23 (1) If the Director files suit within 90 days  
24 from receipt of the written request to commence the  
25 action, no other action may be brought unless the

1 action brought by the Director is dismissed without  
2 prejudice.

3 (2) If the Director does not file suit within 90  
4 days from receipt of the written request to com-  
5 mence the action, the person requesting the action  
6 may proceed to file a civil action.

7 (3) The time period within which a civil action  
8 shall be commenced shall be tolled from the date of  
9 receipt by the Director of the written request to ei-  
10 ther the date that the civil action is dismissed with-  
11 out prejudice, or for 150 days, whichever is later,  
12 but only for a civil action brought by the person who  
13 requested the Director to commence the action.

14 (b) ALLOCATION OF CIVIL PENALTIES.—If a judg-  
15 ment is entered against the defendant or defendants in  
16 an action brought pursuant to this section, or the matter  
17 is settled, amounts received as civil penalties or pursuant  
18 to a settlement of the action shall be allocated as follows:

19 (1) If the action was brought by the Director  
20 upon a request made by a person pursuant to sub-  
21 section (a), the person who made the request shall  
22 be entitled to 15 percent of the civil penalties.

23 (2) If the action was brought by the person who  
24 made the request pursuant to subsection (a), that  
25 person shall receive an amount the court determines

1 is reasonable for collecting the civil penalties on be-  
2 half of the government. The amount shall be not less  
3 than 25 percent and not more than 50 percent of  
4 the proceeds of the action and shall be paid out of  
5 the proceeds.

6 **TITLE V—RELATION TO OTHER**  
7 **LAW**

8 **SEC. 501. EFFECTIVE DATE.**

9 (a) IN GENERAL.—This Act shall apply beginning on  
10 the date that is 1 year after the date of the enactment  
11 of this Act.

12 (b) AUTHORITY TO PROMULGATE REGULATIONS AND  
13 TAKE CERTAIN OTHER ACTIONS.—Nothing in subsection  
14 (a) affects the authority of the Agency to take an action  
15 expressly required by a provision of this Act to be taken  
16 before the effective date described in such subsection.

17 **SEC. 502. RELATION TO OTHER FEDERAL LAW.**

18 Nothing in this Act shall be construed to modify,  
19 limit, or supersede the operation of any privacy or security  
20 provision in the following:

21 (1) Section 552a of title 5, United States Code  
22 (commonly known as the “Privacy Act of 1974”).

23 (2) The Right to Financial Privacy Act of 1978  
24 (12 U.S.C. 3401 et seq.).

1           (3) The Fair Credit Reporting Act (15 U.S.C.  
2       1681 et seq.).

3           (4) The Fair Debt Collection Practices Act (15  
4       U.S.C. 1692 et seq.).

5           (5) The Children’s Online Privacy Protection  
6       Act of 1998 (15 U.S.C. 6501 et seq.).

7           (6) Title V of the Gramm-Leach-Bliley Act (15  
8       U.S.C. 6801 et seq.).

9           (7) Chapter 119, 123, or 206 of title 18,  
10      United States Code.

11          (8) Section 444 of the General Education Pro-  
12      visions Act (20 U.S.C. 1232g) (commonly known as  
13      the “Family Educational Rights and Privacy Act of  
14      1974”).

15          (9) Section 445 of the General Education Pro-  
16      visions Act (20 U.S.C. 1232h).

17          (10) The Privacy Protection Act of 1980 (42  
18      U.S.C. 2000aa et seq.).

19          (11) The regulations promulgated under section  
20      264(c) of the Health Insurance Portability and Ac-  
21      countability Act of 1996 (42 U.S.C. 1320d–2 note),  
22      as those regulations relate to—

23              (A) a person described in section 1172(a)  
24              of the Social Security Act (42 U.S.C. 1320d–  
25              1(a)); or

1 (B) transactions referred to in section  
2 1173(a)(1) of the Social Security Act (42  
3 U.S.C. 1320d–2(a)(1)).

4 (12) The Communications Assistance for Law  
5 Enforcement Act (47 U.S.C. 1001 et seq.).

6 (13) Section 222, 227, 338, or 631 of the Com-  
7 munications Act of 1934 (47 U.S.C. 222, 227, 338,  
8 or 551).

9 (14) The E-Government Act of 2002 (44  
10 U.S.C. 101 et seq.).

11 (15) The Paperwork Reduction Act of 1995 (44  
12 U.S.C. 3501 et seq.).

13 (16) The Federal Information Security Manage-  
14 ment Act of 2002 (44 U.S.C. 3541 et seq.).

15 (17) The Currency and Foreign Transactions  
16 Reporting Act of 1970, as amended (commonly  
17 known as the “Bank Secrecy Act”) (12 U.S.C.  
18 1829b and 1951–1959, 31 U.S.C. 5311–5314 and  
19 5316–5332), including the International Money  
20 Laundering Abatement and Financial Anti-Ter-  
21 rorism Act of 2001, title III of Public Law 107–56,  
22 as amended.

23 (18) The National Security Act of 1947 (50  
24 U.S.C. 3001 et seq.).

1           (19) The Foreign Intelligence Surveillance Act  
2 of 1978, as amended (50 U.S.C. 1801 et seq.).

3           (20) The Civil Rights Act of 1964 (Public Law  
4 88–352, 78 Stat. 241).

5           (21) The Americans with Disabilities Act (42  
6 U.S.C. 12101 et seq.).

7           (22) The Fair Housing Act (42 U.S.C. 3601 et  
8 seq.).

9           (23) The Consumer Financial Protection Act of  
10 2010 (12 U.S.C. 5481 et seq.).

11           (24) The Equal Credit Opportunity Act (15  
12 U.S.C. 1691 et seq.).

13           (25) The Age Discrimination in Employment  
14 Act (29 U.S.C. 621 et seq.).

15           (26) The Genetic Information Nondiscrimina-  
16 tion Act (Public Law 110–233, 122 Stat. 881).

17           (27) Subpart A of part 46 of title 45, Code of  
18 Federal Regulations (commonly known as the “Com-  
19 mon Rule”).

20           (28) The Driver’s Privacy Protection Act of  
21 1994 (18 U.S.C. 2721 et seq.).

22           (29) The Video Privacy Protection Act (18  
23 U.S.C. 2710 et seq.).

24           (30) Chapters 61, 68, 75, and 76 of the Inter-  
25 nal Revenue Code of 1986.

1           (31) Section 1106 of the Social Security Act  
2           (42 U.S.C. 1306).

3           (32) The Stored Communications Act (18  
4           U.S.C. 2701 et seq.).

5           (33) Any other privacy or information security  
6           provision of Federal law.

7   **SEC. 503. RELATION TO STATE LAW.**

8           This Act, and any amendment, standard, rule, re-  
9           quirement, assessment, or regulation promulgated under  
10          this Act, does not annul, alter, affect, or exempt any per-  
11          son subject to the provisions of this Act from complying  
12          with the laws of any State or political subdivision of a  
13          State with respect to privacy or consumer protection, ex-  
14          cept to the extent that those laws are inconsistent with  
15          any provisions of this Act, and then only to the extent  
16          of the inconsistency. For purposes of this section, a law  
17          of a State or political subdivision of a State is not incon-  
18          sistent with this Act if the protection such law affords any  
19          consumer is greater than the protection provided by this  
20          Act.

21   **SEC. 504. SEVERABILITY.**

22          If any provision of this Act or the amendments made  
23          by this Act, or the application thereof, is held unconstitu-  
24          tional or otherwise invalid, the validity of the remainder

1 of the Act, the amendments, and the application of such  
2 provision shall not be affected thereby.

3 **TITLE VI—NIST AND NSF**  
4 **ACTIVITIES**

5 **SEC. 601. NATIONAL INSTITUTE OF STANDARDS AND TECH-**  
6 **NOLOGY PRIVACY RESEARCH AND DEVELOP-**  
7 **MENT.**

8 Section 2 of the National Institute of Standards and  
9 Technology Act (15 U.S.C. 272) is amended by adding  
10 at the end the following:

11 “(f) PRIVACY RISK MANAGEMENT RESEARCH.—In  
12 carrying out the activities under subsection (c)(19), the  
13 Director shall, to the extent practicable and appropriate—

14 “(1) develop, and periodically update, in col-  
15 laboration with appropriate Federal agencies, indus-  
16 try, State, local, and Tribal governments, civil soci-  
17 ety, other nonprofit organizations, and the Informa-  
18 tion Security and Privacy Advisory Board, a privacy  
19 risk management framework that covers risks associ-  
20 ated with data processing and that shall—

21 “(A) identify voluntary, consensus-based  
22 technical standards, guidelines, best practices,  
23 methodologies, procedures, and processes for—



1 “(i) developing privacy-enhanced in-  
2 formation systems and networks, including  
3 emerging technologies; and

4 “(ii) assessing and mitigating privacy  
5 risks to help organizations protect individ-  
6 uals’ privacy in information systems and  
7 networks;

8 “(B) establish common definitions and  
9 characterizations for aspects of privacy risk  
10 management;

11 “(C) provide case studies and risk profiles  
12 of framework implementation;

13 “(D) provide guidance to enable organiza-  
14 tions to use the framework to meet privacy re-  
15 quirements from Federal, State, local, and  
16 Tribal governments and international policy-  
17 makers;

18 “(E) incorporate voluntary, consensus-  
19 based technical standards and best practices;

20 “(F) facilitate use by regulators and mar-  
21 kets with the aim of reducing barriers to trade;  
22 and

23 “(G) not prescribe or otherwise require the  
24 use of specific information or communications  
25 technology products or services;

1           “(2) carry out research associated with miti-  
2           gating privacy risks associated with information sys-  
3           tems and networks, including to inform periodic up-  
4           dates to the privacy risk management framework de-  
5           veloped pursuant to paragraph (1);

6           “(3) in consultation with the Director of the  
7           Digital Privacy Agency, the Federal Trade Commis-  
8           sion, and other related sector-specific risk manage-  
9           ment agencies, support the development of guidance  
10          and risk profiles to help organizations utilize the pri-  
11          vacy risk management framework developed pursu-  
12          ant to paragraph (1), to the extent practicable, to  
13          adopt privacy requirements and regulations estab-  
14          lished by the Federal Government, States, and inter-  
15          national policymakers;

16          “(4) support activities to improve the efficacy  
17          and applicability of privacy-preserving computing,  
18          de-identification techniques and processes, and other  
19          technological means of mitigating individuals’ pri-  
20          vacy risks by enhancing predictability, manage-  
21          ability, disassociability, and confidentiality;

22          “(5) support and strategically engage in the de-  
23          velopment of voluntary, consensus-based technical  
24          standards for privacy-enhanced systems and net-  
25          works, including international technical standards,

1 through open, transparent, and consensus-based  
2 processes; and

3 “(6) conduct such other activities as determined  
4 necessary by the Director to help public and private  
5 sector organizations mitigate the privacy risks asso-  
6 ciated with information systems and networks.”.

7 **SEC. 602. NATIONAL PRIVACY AWARENESS AND EDU-**  
8 **CATION INITIATIVE.**

9 (a) NATIONAL PRIVACY AWARENESS AND EDU-  
10 CATION INITIATIVE.—The Director of the National Insti-  
11 tute of Standards and Technology, in consultation and col-  
12 laboration with relevant Federal agencies, State, local, and  
13 Tribal governments, industry, educational institutions,  
14 civil society, and other nonprofit organizations, as appro-  
15 priate, shall carry out privacy-related education and public  
16 awareness activities, including—

17 (1) the widespread dissemination of privacy-re-  
18 lated technical standards and best practices identi-  
19 fied by the Director;

20 (2) efforts to make privacy-related technical  
21 standards and best practices usable by individuals,  
22 small-to-medium-sized businesses, educational insti-  
23 tutions, and State, local, and Tribal governments;

1           (3) activities to increase the awareness of pri-  
2       vacy risks, individual privacy rights, and responsibil-  
3       ities; and

4           (4) supporting the development of technical  
5       standards and best practices to describe privacy-re-  
6       lated tasks, knowledge, skills, abilities, competencies,  
7       and work roles to guide career development, edu-  
8       cation, and training activities in industry, academia,  
9       nonprofit organizations, and the Federal Govern-  
10      ment, including support for credentialing.

11      (b) CONSIDERATIONS.—In carrying out the authority  
12      described in subsection (a), the Director of the National  
13      Institute of Standards and Technology, in consultation  
14      with appropriate Federal agencies, shall leverage, to the  
15      extent practicable, the national cybersecurity awareness  
16      and education program under section 303 of the Cyberse-  
17      curity Enhancement Act of 2014 (15 U.S.C. 7443).

18      (c) BIENNIAL BRIEFINGS.—Not later than one year  
19      after the date of the enactment of this Act and biennially  
20      thereafter, the Director of the National Institute of Stand-  
21      ards and Technology shall brief the Committee on Com-  
22      merce, Science, and Transportation of the Senate and the  
23      Committee on Science, Space, and Technology of the  
24      House of Representatives on the activities carried out pur-  
25      suant to subsection (a).

1 (d) AUTHORIZATION OF APPROPRIATIONS.—There is  
2 authorized to be appropriated to carry out this section  
3 \$3,000,000 for each of fiscal years 2024 through 2028.

4 **SEC. 603. NATIONAL SCIENCE FOUNDATION PRIVACY RE-**  
5 **SEARCH.**

6 The Director of the National Science Foundation  
7 shall make awards on a competitive basis to institutions  
8 of higher education or non-profit organizations (or con-  
9 sortia of such institutions or organizations) to support  
10 multidisciplinary and transdisciplinary socio-technical re-  
11 search to design, prototype, and translate to practice pri-  
12 vacy-preserving technologies and increase understanding  
13 of the human, social, behavioral, and economic dimensions  
14 of such potential technologies, including research on the  
15 following:

16 (1) Public understanding, expectations, and  
17 perspectives on privacy.

18 (2) Consumer privacy rights, including right to  
19 access, correction, deletion, data portability, indi-  
20 vidual autonomy, impermanence, and to be in-  
21 formed.

22 (3) Privacy governance and transparency, in-  
23 cluding notice and consent processes and the efficacy  
24 of privacy policies.

1           (4) Empowering consumers for data ownership  
2           and control.

3           (5) Privacy by design.

4           (6) Privacy-preserving automated decision-mak-  
5           ing systems and human review of automated deci-  
6           sion-making systems.

7           (7) Ensuring privacy in consumer surveillance  
8           systems.

9           (8) User interfaces, including design elements  
10          that deliberately obscure, mislead, coerce, or deceive  
11          consumers.

12          (9) Privacy implications of emerging tech-  
13          nologies.

14          (10) Incentives to implement privacy protec-  
15          tions.